VIRGINIA LAW REVIEW ONLINE

VOLUME 110 MARCH 2024 52–69

***ESSAY***

# CYBER VULNERABILITIES AS TRADE SECRETS

*Samantha L. Blond**

*Can a cybersecurity vulnerability—like a bug in code or a backdoor into a system—be a trade secret? Claiming a flaw as a trade secret may sound strange. Usually, talk of trade secrets conjures up images of scientists in laboratories or complex computer algorithms. But nothing in the definition of a trade secret excludes vulnerabilities. As the electronic theft of company secrets increases, recognizing cyber vulnerabilities as trade secrets could play an important role in safeguarding business information. For companies that depend on trade secret protections, increased digitalization means that their trade secrets may be exposed. And this exposure could result not only in diminished legal protections but also in a devastating loss of company profits, strategic advantage, or cutting-edge research. This Essay proposes that recognizing cyber vulnerabilities as trade secrets can limit those harms and protect important company information.*

* J.D. Candidate, University of Virginia School of Law (expected 2024). Thank you to John Czubek for invaluable feedback and support and to the editors of the *Virginia Law Review* for their thoughtful suggestions.

## INTRODUCTION

Every year, trade secret theft costs American businesses between $225 billion and $600 billion.[1] Some of the thefts are perpetrated from the inside, like by a disgruntled employee who takes confidential files with him to his next job. But a significant portion of this figure comes from cyber espionage—digitally stealing confidential information or trade secrets from a commercial entity.[2] The digitalization of business records and data assist this form of cyber theft.[3] No longer do thieves need to break into a company's offices and sneak out with physical files. Now, the crime can happen from anywhere, including the other side of the world.[4] And as companies increase the amount of information they store digitally, "they have more bits and bytes worth stealing."[5]

Accompanying this increase in corporate espionage is an increase in the kinds of businesses targeted. The world of corporate spying is "no longer cent[e]red on a few 'sensitive' industries, such as defen[s]e and pharmaceuticals."[6] Any business is at risk of having its proprietary information electronically stolen. Instead of a rarity, corporate espionage has "become a general business risk."[7]

On top of the direct economic costs of corporate spying, this increase in cyber espionage greatly reduces companies' incentives for innovation

[1] Fed. Bureau of Investigation, Executive Summary—China: The Risk to Corporate America (2019), https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf/view [https://perma.cc/93BF-FGZR].

[2] See, e.g., Nicole Sganga, Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies, CBS News (May 4, 2022, 12:01 AM), https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/ [https://perma.cc/WT93-T5HL] (noting that "[t]he CCP continues to increase its theft of U.S. technology and intellectual property" via hacking operations).

[3] Tim Maurer & Arthur Nelson, The Global Cyber Threat, Fin. & Dev. 24, 25 (Mar. 2021), https://www.imf.org/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems-maurer [https://perma.cc/6DN4-3YQR].

[4] See, e.g., Phil Mercer, China Accused of Economic Espionage on an Unprecedented Scale, VOA News: East Asia (Oct. 18, 2023, 2:39 AM), https://www.voanews.com/a/china-accused-of-economic-espionage-on-an-unprecedented-scale/7315625.html [https://perma.cc/5ZPY-K4EV].

[5] Corporate Espionage Is Entering a New Era, Economist (May 30, 2022), https://www.economist.com/business/2022/05/30/corporate-espionage-is-entering-a-new-era [https://perma.cc/8NJ3-S4T8].

[6] Id.

[7] Id.

and investment.[8] And understandably so. There is less incentive to devote resources to research and development if that research, or any related proprietary information, could be compromised in a cyberattack. A competitor hiring a hacker to break into your system and steal your cutting-edge research is the modern-day version of a competitor hiring a photographer to take aerial photographs of your company's new factory from an airplane. (Yes, that actually happened.)[9] A foreign government may target American companies' data to help their own businesses "catch up with advanced U.S. technology."[10] Or a cybercriminal may target your data in the hopes of selling it to a third party for a profit.[11] Given the range of threats, keeping trade secrets "safely locked in the digital vault can be devilishly difficult."[12]

Fortunately for companies, trade secret law has developed rapidly over the last few decades to provide robust protection against these thefts. The Economic Espionage Act was passed in 1996 to "protect the trade secrets of all businesses operating in the United States, foreign and domestic alike, from economic espionage and trade secret theft and deter and punish those who would intrude into, damage, or steal from computer networks."[13] The Computer Fraud and Abuse Act, most recently amended in 2008, allows for both criminal charges and civil suits against anyone who breaks into a computer "without authorization or exceeding authorized access."[14] Nearly all fifty states have adopted the Uniform Trade Secrets Act ("UTSA"),[15] and Congress passed a federal version of the UTSA—the Defend Trade Secrets Act—in 2016.[16] So if a company's

[8] Steve Morgan, Global Cybercrime Damages Predicted to Reach $6 Trillion Annually by 2021, Cybercrime Mag. (Oct. 26, 2020), https://cybersecurityventures.com/annual-cybercrime-report-2020/ [https://perma.cc/JG3C-Q8WL].

[9] See E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970).

[10] Eamon Javers, Inside China's Spy War on American Corporations, CNBC (June 21, 2023, 9:10 PM), https://www.cnbc.com/2023/06/21/inside-chinas-spy-war-on-american-corporations.html [https://perma.cc/LXB2-3MCU].

[11] See, e.g., United States v. Genovese, 409 F. Supp. 2d 253, 255 (S.D.N.Y. 2005) (describing defendant's charges for attempting to resell Microsoft source code on his personal website).

[12] Corporate Espionage Is Entering a New Era, supra note 5.

[13] President William J. Clinton, Statement on Signing the Economic Espionage Act of 1996, 32 Weekly Comp. Pres. Doc. 2040 (Oct. 11, 1996), *reprinted in* 1996 U.S.C.C.A.N. 4034.

[14] 18 U.S.C. § 1030(a)(1).

[15] Trade Secrets Act Enactment Map, Unif. L. Comm'n, https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 [https://perma.cc/ML7V-BSCT] (last visited Feb. 26, 2024).

[16] Defend Trade Secrets Act, Pub. L. No. 114-153, 130 Stat. 376 (2016).

top-secret formula is stolen, the legal system affords the company a variety of ways to remedy the issue.

But the problem of corporate espionage is not limited to stealing data or research outright. Though companies spent $219 billion globally on cybersecurity defenses in 2022,[17] there is no such thing as perfect cybersecurity, meaning that vulnerabilities—weaknesses in a system that can be exploited by an attacker—exist in any system.[18] Rather than hacking into a system and selling the data or information located within, some cybercriminals try to monetize these flaws by selling hacking tools, hidden exploits, or discovered system vulnerabilities on the black market.[19] This market for previously undiscovered software flaws (otherwise known as zero-day vulnerabilities) is of particular concern because, unlike data theft, it is unregulated.[20]

Currently, there is a private market for weeding cybersecurity vulnerabilities out of companies' systems. Some cyber specialists, often dubbed "white hat hackers," search company systems and equipment for vulnerabilities and report their findings to the company, sometimes for a small reward.[21] More proactive companies hire hacking specialists to find weak spots in their systems so they can address these issues before they are exploited.[22]

But the private market goes both ways: just as some hackers choose to sell their findings back to the company whose system is at risk, others

[17] Matt Kapko, Global Cybersecurity Spending to Top $219B This Year: IDC, Cybersecurity Dive (Mar. 17, 2023), https://www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/ [https://perma.cc/6TV9-D7QT].

[18] Jay Pil Choi, Chaim Fershtman & Neil Gandal, Network Security: Vulnerabilities and Disclosure Policy, 58 J. Indus. Econ. 868, 869 (2010).

[19] See, e.g., Kate O'Flaherty, Notorious Hacking Forum and Black Market Darkode is Back Online, Forbes (Apr. 10, 2019, 12:06 PM), https://www.forbes.com/sites/kateoflahertyuk/2019/04/10/notorious-hacking-forum-darkode-is-back-online/ [https://perma.cc/LX4Y-HY8J] (discussing a site on the black market which "serves as a venue for the sale & trade of hacking services, botnets, malware, and illicit goods and services").

[20] Tom Gjelten, In Cyberwar, Software Flaws are a Hot Commodity, NPR (Feb. 12, 2013, 3:25 AM), https://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity#:~:text=In%20the%20context%20of%20escalating,inside%20his%20enemy%27s%20computer%20network [https://perma.cc/JT9J-NZSL].

[21] Chris Teague, White Hat Hacker Cracked Toyota's Supplier Portal, Autoblog (Feb. 8, 2023, 9:35 AM), https://www.autoblog.com/2023/02/08/white-hat-hacker-toyota-supplier-portal/ [https://perma.cc/B8V2-7NPE].

[22] David Rudin, Safety Net: Hackers for Hire Help Companies Find Their Weak Spots, Fin. Post (Mar. 3, 2023), https://financialpost.com/cybersecurity/hackers-help-companies-find-weak-spots [https://perma.cc/HPV2-H3D9].

choose to sell the information to competitor companies, foreign governments, or other interested parties.[23] And for good reason—the price on the black market for vulnerabilities is often ten to one hundred times higher than on the white market.[24] As the black market for vulnerabilities grows, companies' proprietary information is put increasingly at risk.

Unfortunately, due to the lack of regulation of this market, there has been little stopping the growth in corporate espionage. Existing suggestions in academic literature for tackling the global trade in zero-day vulnerabilities include criminalization,[25] regulation through export controls,[26] and "increasing the payouts offered on the white market through a combination of liability protections, tax benefits, and subsidies."[27] This Essay offers a simple alternative—or supplement—to these options: protecting cyber vulnerabilities through trade secret law.

By correctly applying trade secret law to zero-day vulnerabilities, companies will be afforded many options to protect their cybersecurity weaknesses from falling into the hands of their competitors or the public. A company whose system has been poked and prodded for vulnerabilities could bring trade secret claims under the applicable law, which could award them not only damages but also an injunction to prevent disclosure or use of the weakness. Federal trade secret law also allows for courts to issue warrants for property seizure, which could prevent the offending individual or organization not only from disseminating the vulnerability but also from conducting further operations.[28] Under the Economic Espionage Act or Computer Fraud and Abuse Act, an offending hacker—or competitor who knowingly uses stolen information—could be held criminally liable.[29] Trade secret law provides companies with many powerful tools for combatting the growing vulnerability black market. By treating vulnerabilities as trade secrets, the legal system will provide companies with far more protections for their systems' weaknesses than

[23] Andi Wilson, Ross Schulman, Kevin Bankston & Trey Herr, New Am., Cybersecurity Initiative, Open Tech. Inst., Bugs in the System: A Primer on the Software Vulnerability Ecosystem and Its Policy Implications 15–18 (2016), https://www.newamerica.org/oti/policy-papers/bugs-system/ [https://perma.cc/53AM-DYRN].

[24] Lillian Ablon, Martin C. Libicki & Andrea A. Golay, Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar 26 (2014).

[25] Mailyn Fidler, Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis, 11 I/S: J.L. & Pol'y for Info. Soc'y 405, 424 (2015).

[26] Id. at 432.

[27] Nathan Alexander Sales, Privatizing Cybersecurity, 65 UCLA L. Rev. 620, 620 (2018).

[28] 18 U.S.C. § 1836(b)(2)(A)(i).

[29] Id. §§ 1832, 1030(a), (c).

currently exist. This, in turn, will help protect their underlying research and data.

One case has contemplated the application of cybercrime law to system vulnerabilities. In 2008, three undergraduate students at the Massachusetts Institute of Technology ("MIT") planned to present research at a cybersecurity conference that exposed "weaknesses in common subway fare collection systems," particularly the Massachusetts Bay Transportation Authority ("MBTA").[30] Their demonstration promised to "present several attacks to completely break the CharlieCard" (the MBTA's subway card), "release several open source tools [they] wrote to perform these attacks," and reveal "how [they] broke these systems."[31]

Ironically, the students' presentation included a slide with the text: "What this talk is *not*: evidence in court (hopefully)."[32] But before they could give their presentation, the MBTA sued, alleging the students' research violated the Computer Fraud and Abuse Act ("CFAA").[33] Though the MBTA was initially granted a temporary restraining order, the U.S. District Court for the District of Massachusetts later denied the MBTA's request for a preliminary injunction and dissolved the restraining order, finding that discussing the system's vulnerabilities was likely not the sort of "transmission" covered by the CFAA.[34]

But the District of Massachusetts's ruling is not the end-all-be-all for legal protection of vulnerabilities. The MBTA brought suit under the Computer Fraud and Abuse Act, not the Uniform Trade Secrets Act, as Massachusetts had yet to adopt the UTSA.[35] Nearly a decade later, the Massachusetts legislature passed the Massachusetts Uniform Trade Secrets Act, bringing it up to speed with forty-eight other states.[36]

[30] Complaint at 1, 7, Mass. Bay Transp. Auth. v. Anderson, No. 08-cv-11364 (D. Mass. Aug. 8, 2008).

[31] Id. at 7.

[32] Complaint, Exhibit 7 at 3, *Mass. Bay Transp. Auth.*, No. 08-cv-11364 (emphasis added).

[33] Complaint, supra note 30, at 12.

[34] Transcript of Motion Hearing at 60, 65, *Mass. Bay Transp. Auth.*, No. 08-cv-11364 (D. Mass. Aug. 19, 2008).

[35] Complaint, supra note 30, at 12.

[36] Aaron Nicodemus, Massachusetts Adopts Uniform Trade Secret Law, Bloomberg L. (Aug. 16, 2018, 5:29 PM), https://news.bloomberglaw.com/ip-law/massachusetts-adopts-uniform-trade-secrets-law [https://perma.cc/FYS3-QAG4]. New York has not adopted the Uniform Trade Secrets Act and instead still relies on common law tort claims. Though North Carolina has not adopted the UTSA, it is counted as one of the forty-nine because its state

Under the UTSA, the court's decision to dissolve the temporary restraining order and deny preliminary injunctive relief could have come out very differently. A vulnerability or weakness in a company's cybersecurity could qualify as a trade secret under the UTSA. Not only will recognizing vulnerabilities as trade secrets protect against innocent disclosures of proprietary information, as in the MBTA case, but it will also help reduce the growing threat of cyber espionage and weaken the market for vulnerabilities.

Part I of this Essay explains why vulnerabilities ought to qualify for trade secret protections under the definition of a trade secret in the Uniform Trade Secrets Act. Part II makes a normative argument for including vulnerabilities in trade secret protection. The Essay concludes by briefly revisiting the MBTA case to show how affording vulnerabilities protection under the UTSA would prevent future harms to the MBTA.

## I. CYBERSECURITY VULNERABILITIES AND THE DEFINITION OF TRADE SECRETS

Given the breadth of coverage extended by the UTSA, cybersecurity vulnerabilities should qualify for trade secret protection. The UTSA defines a trade secret as

> 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.[37]

Thus, to claim a trade secret under the UTSA, the owner must prove (1) the information is of the type covered by the Act, (2) the information is not generally known or readily ascertainable, (3) the information derives independent economic value from its secrecy, and (4) the owner has taken reasonable efforts to maintain the secrecy of the information.[38]

trade secrets law is very similar to the UTSA. See Christopher T. Zirpoli, Cong. Rsch. Serv., IF12315, An Introduction to Trade Secrets Law in the United States (2023).

[37] Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).

[38] Id.

Just as a company claiming trade secret protection over a top-secret soda recipe must establish each of these four elements, so too must a company claiming trade secret protection over a vulnerability.

### *A. Qualifying Information*

First, a party claiming a trade secret in a vulnerability must establish that the information is protected by the UTSA. The UTSA covers "information, including a formula, pattern, compilation, program, device, method, technique, or process."[39] But it is not limited to the categories listed in the text of the statute. Many courts and scholars agree that an implied "any" precedes the word "information"—thus, *any* information can be covered by the UTSA.[40] A category of information cannot be "excluded from protection as a trade secret because of its inherent qualities."[41] Because trade secret law does not exclude any information as a result of the nature of that information, there is no reason that a cybersecurity vulnerability cannot be the type of "information" contemplated by the UTSA.[42]

Importantly, the UTSA, unlike its common law predecessors, does not require that the information be in use to qualify for trade secret protection.[43] This modification from the definition of trade secret in the Restatement of Torts further expands the types of information that can be protected.[44] And in the case of cybersecurity weaknesses, it means that a plaintiff need not show that the party is in any way "using" the vulnerability, which may be confusing to prove.

---

[39] Id.

[40] See, e.g., Elizabeth A. Rowe & Sharon K. Sandeen, Trade Secret Law: Cases and Materials 2 (3d ed. 2021) (arguing that a trade secret can be virtually any information that is useful in a business as long as it is kept secret).

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

[42] Federal trade secret law, the Defend Trade Secrets Act of 2016 ("DTSA"), defines a trade secret more narrowly than the UTSA. The DTSA only covers "financial, business, scientific, technical, economic, or engineering information," and because it is a federal statute, the information must be sufficiently "related to" interstate or foreign commerce to invoke Congress's Commerce Clause power. 18 U.S.C. § 1839(3). Thus, a plaintiff will have a much harder time claiming a trade secret over a vulnerability under the DTSA than the UTSA. This Essay does not take a position as to whether a vulnerability may be a trade secret under the DTSA.

[43] Compare Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985) (defining a trade secret without specifying a "use" requirement), with the Restatement of Torts § 757 cmt. b (Am. L. Inst. 1939) (defining a trade secret as "consist[ing] of any formula, pattern, device or compilation of information which is *used* in one's business") (emphasis added)).

[44] Id.

The only restriction on information eligible for protection is that the plaintiff must be able to identify its trade secrets with particularity.[45] But this is true for all claimed trade secrets. Just as a party could not broadly claim that its "data" is a trade secret without further specifying *which* data, neither could a company claim that its "general cyber defenses and their weaknesses" are trade secrets. As long as a plaintiff defines with particularity the vulnerability it is claiming as a trade secret, the vulnerability can satisfy this first requirement.

### *B. Secrecy*

The second requirement is secrecy: the subject of a trade secret must not be generally known or readily ascertainable.[46] A thing is not generally known if it is neither known to the public nor widely known within the relevant industry.[47] It is not readily ascertainable if obtaining the information would be challenging or time- and resource-intensive.[48]

Some vulnerabilities may be obvious or widely known, especially if it is a vulnerability that affects multiple companies. For example, if a company relies on a third-party program for its firewall, and it is widely known among the cybersecurity community that said program has a particular flaw, then a company may not be able to claim this flaw as its trade secret. But there are certainly other scenarios in which a vulnerability is not generally known to others and in which identifying the vulnerability would be difficult, expensive, and time-consuming. In these cases, the information should pass the secrecy requirement.

Additionally, the law has recognized that not every element of a trade secret need be secret. Trade secrets frequently contain some elements that by themselves may be in the public domain but together qualify as a trade secret.[49] Whether a vulnerability is secret will vary from case to case, but

[45] See, e.g., Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1252 (N.D. Cal. 1995) ("[T]he secret aspect of [the information claimed as a trade secret] must be defined with particularity.").

[46] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974).

[47] Rowe & Sandeen, supra note 40, at 94.

[48] Microstrategy, Inc. v. Bus. Objects, S.A., 331 F. Supp. 2d 396, 417 (E.D. Va. 2004). Some states that adopted the UTSA removed the readily ascertainable language from the definition and instead allow it to be raised as a defense. Rowe & Sandeen, supra note 40, at 94.

[49] See, e.g., Pyro Spectaculars N., Inc. v. Souza, 861 F. Supp. 2d 1079, 1089–90 (E.D. Cal. 2012) (finding customer lists to be a trade secret even though much of the customer data was generally known to the public).

particularly when discussing zero-days, which are by definition known neither to the programmer nor the public, the secrecy requirement should often be met.

### *C. Independent Economic Value*

Third, a trade secret owner must show that the information "derives independent economic value . . . from not being generally known to . . . other persons."[50] The contours of the independent economic value requirement are debated,[51] but it is generally understood that the trade secret must confer competitive value to its owners.[52] Some courts assume that a trade secret at issue has economic value because otherwise the plaintiff would not waste time and resources bringing a claim.[53] Defendants attempting to attack the economic value requirement of a plaintiff's claim are often fighting a losing battle because courts have set the bar low.[54]

Even if a court wished to inquire into the economic value of a vulnerability, the fact that there is a market for such information should be evidence enough of its value. And there is clear value derived from the information's secrecy—a cybersecurity flaw, if exposed, would leave a company at risk of data theft and trade secret loss. Thus, there is immense competitive value in keeping the flaw a secret.

### *D. Reasonable Efforts to Maintain Secrecy*

Fourth, and most importantly, a trade secret owner must show that it took affirmative steps to protect the thing that it claims as a trade secret.[55] This will likely be the hardest element for a plaintiff alleging a trade secret in a cybersecurity vulnerability to prove. Because many companies are unaware of such vulnerabilities until they are exploited—otherwise, they would patch the weaknesses to protect themselves—defendants would argue that without knowledge of the issue, the company could not take

[50] Unif. Trade Secrets Act § 1(4)(i) (Unif. L. Comm'n 1985).

[51] Eric E. Johnson, Trade Secret Subject Matter, 33 Hamline L. Rev. 545, 557 (2010).

[52] Cy Wakeman, Inc. v. Nicole Price Consulting, LLC, 284 F. Supp. 3d 985, 996 (D. Neb. 2018).

[53] Rowe & Sandeen, supra note 40, at 146.

[54] See, e.g., Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1253 (N.D. Cal. 1995) (finding value even if only to nonexistent potential competitors).

[55] Id.

any affirmative steps to protect the secret.[56] And, if they did know about the vulnerability and chose to do nothing, a court may find such inaction to be unreasonable. Reasonable efforts may require "ongoing assessment and review of [a company's] security plan" to patch vulnerabilities.[57]

But the standard for secrecy is not absolute. Rather, a company need only show that its efforts were reasonable under the circumstances.[58] Because it is impossible to find and fix every vulnerability, as long as the company took steps to tailor its security measures to external threats, a court may find that its efforts were reasonable, even if the specific vulnerability at issue was unknown to the company.[59] There is no "checklist of specific items" that a company must show it performed to merit protection.[60] If it can demonstrate that it did take preventative measures, and it adequately tailored the measures to the trade secret at issue, that may be enough to show reasonableness. The plaintiff could always do more to protect its secret. The question for the court is whether the plaintiff's "failure to do more" was unreasonable.[61]

Additionally, economic considerations may often weigh in favor of finding a company's efforts reasonable. In a Seventh Circuit case, Judge Posner reasoned that if the plaintiff "expended only paltry resources on preventing its [alleged trade secret] from falling into the hands of competitors . . . why should the law . . . bother to provide [the plaintiff] with a remedy?"[62] Conversely, if a plaintiff expends immense resources on cyber defenses—building adequate cybersecurity systems, employing ethical hackers to seek out vulnerabilities, and patching weaknesses where found—why should the law *not* provide plaintiff with a remedy? If it is widely accepted that it is impossible to detect and remove all vulnerabilities (and it is),[63] then companies should not be penalized for

[56] See Incase Inc. v. Timex Corp., 488 F.3d 46, 53 (1st Cir. 2007) (holding that taking these reasonable efforts requires "affirmative steps to preserve the secrecy of the information as against the party against whom the misappropriation claim is made").

[57] Elizabeth A. Rowe, RATs, TRAPs, and Trade Secrets, 57 B.C. L. Rev. 381, 415 (2016).

[58] Learning Curve Toys, Inc. v. PlayWood Toys, Inc., 342 F.3d 714, 725 (7th Cir. 2003) (noting that the reasonable efforts standard "does not require perfection").

[59] Elizabeth A. Rowe, Contributory Negligence, Technology, and Trade Secrets, 17 Geo. Mason L. Rev. 1, 2 (2009) ("While absolute secrecy is not required, the trade secret owner is expected to show that it took efforts reasonable under the circumstances . . . .").

[60] Id. at 3.

[61] Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 177 (7th Cir. 1991).

[62] Id. at 179.

[63] Derek E. Bambauer, Ghost in the Network, 162 U. Pa. L. Rev. 1011, 1020 (2014) (concluding that "vulnerabilities are inevitable"); see also George Finney, The Illusion of

not doing the impossible. The law cannot require a trade secret owner to "guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available."[64] Nor can the law require that, to guarantee trade secret protection, a company expend all of its resources on security measures. Instead, an inquiry into reasonable efforts must balance the degree of secrecy protections against the cost of additional protections.[65] A company could buy every cybersecurity program on the market and pay dozens of experts to constantly mine the system for vulnerabilities, but it would be doing so at the cost of funding other vital aspects of the business. The law "should not require a person or corporation to take unreasonable precautions to prevent another from doing that which he ought not do in the first place."[66] Nor should "[t]he market place . . . deviate far from our mores."[67] In other words, at some point enough is enough. A company should not be penalized for deciding where that point lies (within reason).

Ultimately, whether a plaintiff has taken reasonable efforts is a question of fact. In the case of cybersecurity vulnerabilities, a jury could find that the company took reasonable steps to maintain secrecy. Once the four elements of a trade secret have been established, a plaintiff alleging trade secret misappropriation need only prove that the defendant acquired the information through improper means or disclosed or used the information in violation of an express or implied agreement of confidentiality.[68] For cases involving corporate espionage or hacking, this should be simple to establish.

Because anything can be a trade secret under the UTSA, it is important to recognize that allowing a plaintiff to claim a trade secret in a cybersecurity vulnerability is not expanding existing trade secret law. Rather, if a plaintiff can prove the requisite elements of a trade secret law claim, trade secret law should rightly protect a company's cybersecurity vulnerabilities.

Perfect Cybersecurity, Forbes (Mar. 27, 2018, 8:45 AM), https://www.forbes.com/sites/forbestechcouncil/2018/03/27/the-illusion-of-perfect-cybersecurity/?sh=72f3bfc811f9 [https://perma.cc/X9UT-GQ22] (arguing there is no such thing as perfect cybersecurity).

[64] E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970).

[65] *Rockwell Graphic Sys.*, 925 F.2d at 179.

[66] *Christopher*, 431 F.2d at 1017.

[67] Id.

[68] Unif. Trade Secrets Act § 1(2) (Unif. L. Comm'n 1985).

## II. A NORMATIVE ARGUMENT FOR APPLYING TRADE SECRET LAW TO VULNERABILITIES

Not everyone agrees that vulnerabilities should be protected as trade secrets. Some believe the publication of security vulnerabilities is "critical for scientific advancement, public safety[,] and a robust market for secure technologies."[69] If information about vulnerabilities, like that of the MIT students, cannot be shared publicly, there may be a "chilling effect" on research and publication on such topics.[70] Others may have First Amendment concerns.[71] And because these vulnerabilities could risk businesses' client data or customer information, the public interest may be best served by not protecting the secrecy of vulnerabilities.

Yet, if vulnerabilities are left outside the trade secret umbrella, many of the purposes for trade secret protections are violated. This is especially true given the nature of cybersecurity. Because there is no such thing as perfect cybersecurity, practically every system at every company will have weaknesses. Perhaps more than anything, protecting and safeguarding those weaknesses (or the knowledge of them) is integral to protecting and safeguarding a company's research and data. Additionally, the same public policy concerns that justify trade secret law justify applying trade secret law to vulnerabilities. Even if some of the critics' concerns have merit, the existing contours of trade secret law will cabin the protections provided to vulnerabilities, minimizing any harm to the public. Lastly, recognizing vulnerabilities as trade secrets does not provide them with unlimited protections: sometimes, the First Amendment will require that the information be made public.

### *A. Public Policy Justifications*

The public policy justifications for trade secret protections also apply to cybersecurity vulnerabilities. The strongest such justification is commercial morality—trade secret law penalizes the disclosure or use of trade secrets that are obtained through improper means because to ensure

[69] Letter from Computer Science Professors and Computer Scientists at 1, Mass. Bay Transp. Auth. v. Anderson, No. 08-cv-11364 (D. Mass. Aug. 11, 2008).

[70] Id.

[71] See Sharon K. Sandeen & Ulla-Maija Mylly, Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing, 21 N.C. J.L. & Tech., no. 3, 2020, at 1, 3–4 n.2 (compiling works that discuss the issue of the First Amendment in trade secret law).

innovation, the system must reflect a respect for innovation.[72] This ethical underpinning explains why trade secret law regulates not just illegal acts, but also immoral acts.[73] Though our economic system highly encourages competition, "our devotion to freewheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations."[74]

Just as hacking into a company's system and stealing its data is contrary to commercial morality and fair competition, so too is disclosing or exploiting a company's cyber vulnerabilities. That current regulations do not criminalize the disclosure of such vulnerabilities—instead only criminalizing any hacking that results from it—does not change this evaluation. Selling a company's vulnerabilities on the black market, or hiring a hacker to discover them for you, is improper. These actions "fall below the generally accepted standards of commercial morality and reasonable conduct," which is the standard for trade secret misappropriation.[75] Protecting vulnerabilities as trade secrets furthers the same goals as protecting more conventionally-accepted trade secrets.

Trade secret law is also designed to foster innovation. By allowing inventors to protect the fruits of their labor, trade secret law encourages the funding of research. Companies are more likely to put money into developing new ideas if that output would be protected. But the growing black market for cybersecurity weaknesses is stifling the incentive to invest in research.[76] The greater the risk that the confidential information could be compromised in a cyberattack or hack, the lower the incentive to devote resources to research and development. And though some level of business intelligence is necessary in our economic system, "[o]ur tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."[77] Protecting cyber vulnerabilities as trade secrets is one way to restore faith in corporate investments.

[72] Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) ("The future of the nation depends in no small part on the efficiency of the industry, and the efficiency of the industry depends in no small part on the protection of intellectual property.").

[73] See, e.g., E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) (finding misappropriation where defendants took photos from public airspace).

[74] Id.

[75] Id. (quoting Restatement of Torts § 757, cmt. f at 10–11 (Am. L. Inst. 1939)).

[76] Morgan, supra note 8.

[77] *Christopher*, 431 F.2d at 1016.

It is important to distinguish between vulnerabilities that could be exploited *in the future* and breaches or hacks that have *already occurred*. This Essay is not suggesting that the latter be extended trade secret protections. It would be contrary to the public policy justifications for trade secret law to provide trade secret protection for past breaches, particularly where customer data or personal information is concerned. Extending trade secret protection to past breaches would also conflict with recent legislation that requires publicly traded companies to disclose cybersecurity incidents.[78]

### *B. Trade Secret Law as a Check*

Trade secret protections for vulnerabilities would not allow companies to claim broad swaths of information as trade secrets without limitations any more than trade secret law already does. Just like any trade secret, an entity claiming to possess a trade secret over a vulnerability must be able to prove the requisite elements of a trade secret: (1) the information is of the type that can be a trade secret—which, as already established, is any information under the UTSA; (2) the information is not generally known or readily available; (3) the information has independent economic value; and most importantly, (4) the owner of the information took reasonable efforts to keep it secret.[79] Should a plaintiff fail to provide evidence of any one of these elements, trade secret law will not protect the disclosure or use of the vulnerability.

The standard for injunctive relief also ensures that the application of trade secret law to vulnerabilities does not violate the public interest. When considering whether to grant an injunction—often to limit the use or disclosure of an alleged trade secret—courts are instructed to weigh the public interest.[80] If the public interest in revealing the information outweighs the commercial interests in keeping the information private, the court may deny a plaintiff's request for an injunction.

And, to get an injunction, a plaintiff must also demonstrate a likelihood of success on the merits.[81] Thus, a plaintiff must prove not only that he owns a trade secret, but also that the defendant misappropriated the trade

[78] Cyber Incident Reporting for Critical Infrastructure Act, H.R. 2471, 117th Cong. § 2242(a)(1)(A) (2022).
[79] Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).
[80] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 32 (2008).
[81] Id. at 20.

secret.[82] In the case of corporate espionage, that will often mean demonstrating that the defendant acquired the trade secret through improper means, such as by theft or hacking. The existing bounds of trade secret law will rein in protections of vulnerabilities as they do any other claimed trade secrets.

### *C. The First Amendment*

Nor should First Amendment concerns govern whether vulnerabilities qualify for trade secret protections. In trade secret law, there is often an inherent tension between a defendant's First Amendment freedom of speech (in sharing the confidential information) and a plaintiff's Fifth Amendment right to control its property.[83] In some instances, courts may find that the First Amendment right to share information outweighs a trade secret owner's property interest in its information remaining confidential.[84] Particularly where the plaintiff is seeking to enjoin the defendant from disclosing or publishing the information at issue, the Supreme Court's declaration that prior restraints "may be issued only in rare and extraordinary circumstances" will often restrict a court from enjoining the speech.[85] To justify a prior restraint on speech, the publication of information "must threaten an interest more fundamental than the First Amendment itself."[86] A plaintiff's interest in protecting its "commercial self-interest"—in this scenario, the trade secret—often does not qualify as a more fundamental interest.[87] Thus, when a court finds that the public interest is better served by making the information public than by keeping it private, the First Amendment may trump a plaintiff's right to control the information. But because the scales may *sometimes* tip in favor of public disclosure, this does not mean that vulnerabilities can never be protected; in other cases, the Fifth Amendment may win out.[88]

[82] Roger M. Milgrim, 4 Milgrim on Trade Secrets, § 15.01[1] (2005).

[83] The Supreme Court recognized that a trade secret owner has a property interest in the trade secret, protected by the Fifth Amendment's Takings Clause, in *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 987 (1984).

[84] See, e.g., Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 746 (E.D. Mich. 1999) (holding that the First Amendment did not allow enjoining defendant from posting allegedly misappropriated trade secrets on his website).

[85] Id. at 751 (citing Near v. Minnesota, 283 U.S. 697, 716 (1931)).

[86] Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 227 (6th Cir. 1996).

[87] Id. at 225.

[88] See, e.g., DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 191–92 (Ct. App. 2004).

And even where the interest in making the information public trumps the plaintiff's right to keep it private, this does not mean that the thing the plaintiff is claiming as a trade secret cannot by its nature be a trade secret. The First Amendment is raised as a *defense* to a plaintiff's trade secret claim: Even if the thing were a trade secret, the First Amendment protects the defendant's ability to share the information. An assertion of the defense is irrelevant to the question of whether the thing can be a trade secret.[89] When combined with other legal checks on trade secret claims, the availability of the First Amendment defense should assuage any concerns about applying trade secret protections to vulnerabilities.

## CONCLUSION

In 2023, students who had heard about the MBTA scandal tried to replicate the MIT students' work from fifteen years earlier.[90] To their surprise, they found that the vulnerabilities uncovered by the students in 2008 still existed in the MBTA's system.[91] Using many of the same tricks from the original presentation, the new batch of students hacked the MBTA's CharlieCard system, allowing them to add money to their cards without paying.[92] Essentially, the hack gave the students unlimited free rides.

If the vulnerabilities discovered by the MIT students had been protected as trade secrets back in 2008, court filings would have been sealed and the MIT students would have been enjoined from further disclosing or using the information. The new group of students would not have been able to obtain the information to conduct their own research and carry out further hacks in 2023. The MBTA's business model would be protected, and any threat of lost revenue from hacking would be severely diminished. And if the MBTA successfully petitioned the judge for an injunction in 2008, that injunction would have protected more than just its own system. The MIT students' presentation included a primer on

[89] Pamela Samuelson, Principles for Resolving Conflicts Between Trade Secrets and the First Amendment, 58 Hastings L.J. 777, 779–80 (2007).

[90] Andy Greenberg, Teens Hacked Boston Subway Cards to Get Infinite Free Rides—and This Time, Nobody Got Sued, Wired (Aug. 10, 2023, 2:43 PM), https://www.wired.com/story/mtba-charliecard-hack-defcon-2023/ [https://perma.cc/G52L-YWW8].

[91] Id.

[92] Id.

how to hack transportation systems more generally, implicating the safety, operations, and revenues of subway systems across the globe.[93]

To pull corporate espionage out of its golden era, an era "not unlike the cold war heyday of great-power spookery," more must be done to safeguard companies' proprietary information.[94] While recognizing cyber vulnerabilities as trade secrets will not fully eliminate the cyber espionage problem, it is a start. If a plaintiff can demonstrate the requisite elements of a claim and if the protections do not violate the public interest, the law should not withhold trade secret protections from vulnerabilities.

[93] Complaint, Exhibit 7 at 38–84, Mass. Bay Transp. Auth. v. Anderson, No. 08-cv-11364 (D. Mass. Aug. 8, 2008).

[94] Corporate Espionage Is Entering a New Era, supra note 5.