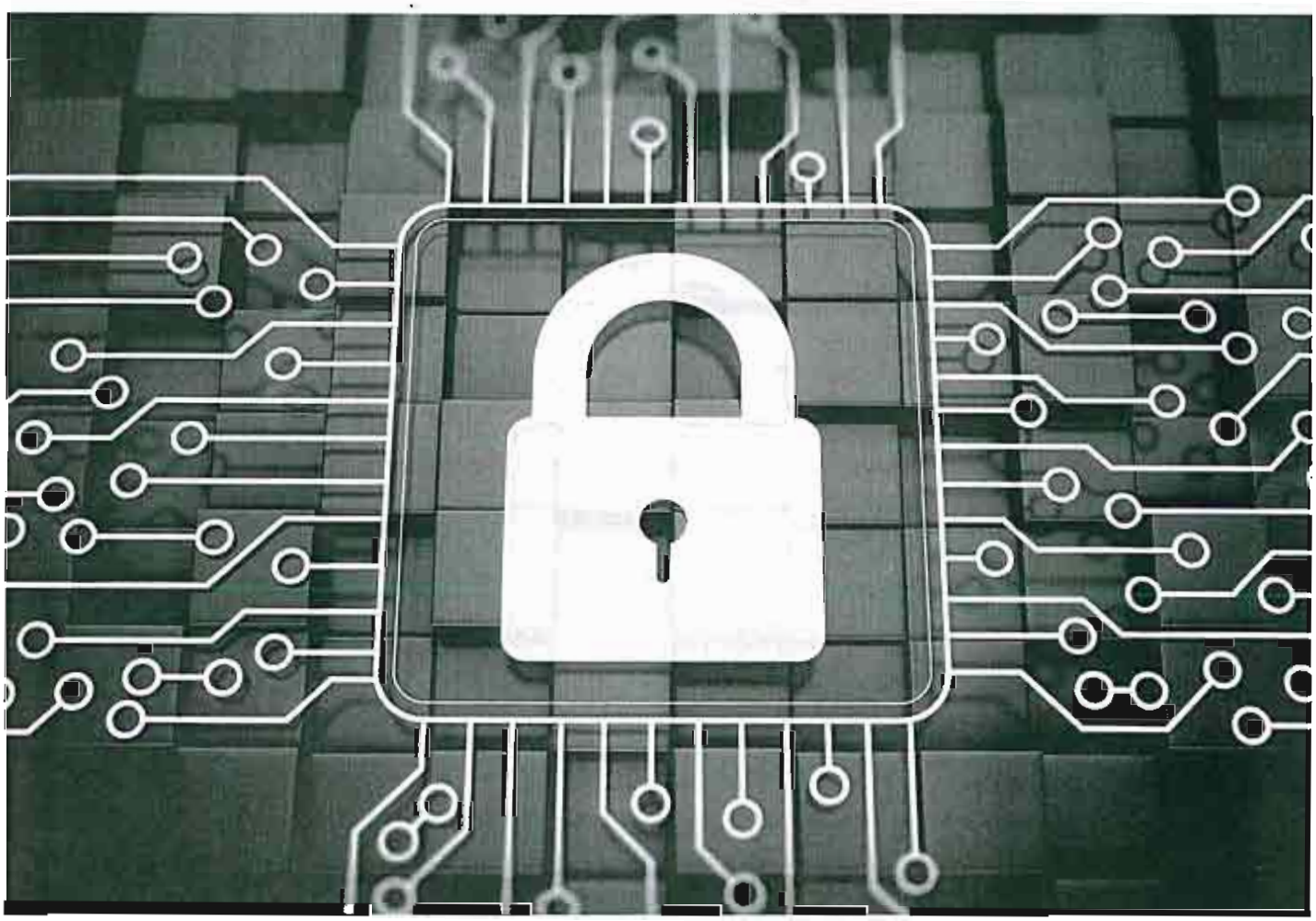
# Seize the Day, or at Least the Trade Secrets

## Protecting Trade Secrets Against Cyber Theft Using the New Jersey Trade Secret Act and the Defend Trade Secrets Act

by John A. Stone



### "For as long as there has been commerce, there has been espionage."[1]

In the early 1700s, for example, Pére d'Entrecalles, a French Jesuit missionary, reportedly stole "secret techniques for manufacturing ceramic" materials, and in the 1800s the "London-based East India Co. hired Scottish botanist and adventurer Robert Fortune to smuggle" "tea's plants, seeds and secrets out of China and into British-ruled India."[2]

As if Fortune's name was not ironic enough, China, the victim of many early misappropriations, is now recognized as one of the biggest practitioners of corporate espionage.[3]

Now that electronic storage and communication have become commonplace, both global corporations and local

businesses should protect their trade secrets. The relatively new New Jersey Trade Secrets Act (NJTSA)[4] and the just-enacted federal Defend Trade Secrets Act (DTSA)[5] provide protection to victims of trade secret theft, including possible seizure of stolen information—a cutting-edge remedy in the ever-evolving world of computer hacking and cybersecurity.[6]

## Cyber Theft of Trade Secrets

"The United States is frequently described as being the nation with the greatest susceptibility to cyber attacks due to both the high number of insufficient networks and the presence of valuable—in some cases world-leading—trade secrets."[7] Indeed, trade secret theft "costs American companies billions of dollars each year,"[8] and "can also force companies to 'lay off employees, to close factories, to lose sales and profits, to experience a decline in competitive position and advantage—or even to go out of business.'"[9]

Companies of all sizes can be damaged by cyber theft.[10]

> Trade secret theft frequently occurs in the United States in industries with high concentrations of technology and research and development activities. The most visible fields that are targeted are: aerospace, biotechnology, computer software and hardware, transportation and engine technology, defense technology, telecommunications, energy research, advanced materials and coatings, stealth technologies, lasers, manufacturing processes, and semiconductors.[11]

"One major reason for the prevalence of trade secret theft is the almost universal use of computers in daily business operations."[12]

> Although technology has made it easy to store vast amounts of data constituting trade secret information electronically, the internet and the rise of cyber intrusions into computer systems and networks have created a storm perfectly ripe for corporate espionage and trade secret misappropriation.[13]
>
> The reliance on computers and the Internet has enabled criminals to instantaneously steal massive quantities of sensitive information while simultaneously evading detection. For employees, the use of computers is one of the most innovative workplace transformations. For employers, computers in the workplace confer substantial benefits by allowing for greater connectivity between enterprises and individuals. Increased connectivity is a double-edged sword. While the use of passwords, firewalls, and encryption to protect network data is certainly advised where applicable, these measures cannot safeguard confidential and proprietary information in every instance.[14]

Indeed, "[t]here is good reason to believe that many trade secret misappropriation incidents are tied to cybersecurity breaches."[15]

## The New Jersey Trade Secrets Act

At least 48 states, including New Jersey, and the District of Columbia, have enacted a version of the Uniform Trade Secrets Act (UTSA).[16]

The NJTSA defines "trade secret" as "information...without regard to form, including a formula, pattern, business data compilation, program, device, method, technique, design, diagram, drawing, invention, plan, procedure, prototype or process," that has economic value, "actual or potential," as a result of not being known to others who might derive economic value from its use.[17]

> A "trade secret" (1) "[d]erives 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 (2) that the holder reasonably endeavors to maintain as confidential.[18]

Information is not a trade secret under the NJTSA unless it has economic value and/or provides competitive advantage.

### *Misappropriation Under the NJTSA*

Under the NJTSA, "misappropriation" of a trade secret includes:

> 1. Acquisition of a trade secret of another by a person who knows or has reason to know that a person acquired the trade secret by improper means; or
> 2. Disclosure or use of a trade secret of another without express or implied consent of the trade secret owner 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 the knowledge of the trade secret was derived or acquired through improper means; or
>    c. Before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired through improper means.[19]

Misappropriation includes the "breach of an express or implied duty to maintain the secrecy of, or to limit the use or disclosure, of a trade secret," as well as "any access that is unauthorized or exceeds the scope of authorization."[20]

Improper means, in turn, include "the theft, bribery, misrepresentation, breach or inducement of a breach of an express or implied duty to maintain the secrecy of, or to limit the use or disclosure of, a trade secret, or espionage through electronic or other means, access that is unauthorized or exceeds the scope of authorization, or other means that violate a person's rights under the laws of this State."[21] Proper

means, by contrast, include discovery by independent invention, reverse engineering, or under a license from the owner of the trade secret, as well as observation of the information in public use or on public display, and obtaining the trade secret from published literature.[22]

*Non-Seizure Remedies Under the NJTSA*

The NJTSA enables parties to obtain an injunction to prevent actual or even threatened misappropriation for a reasonable period of time, and to eliminate commercial advantage flowing from a misappropriation.[23]

If exceptional circumstances exist, future use of a trade secret may be conditioned upon payment of a reasonable royalty for the period of time for which use could have been prohibited.[24] The amount of that royalty is fact-sensitive and may require evidence and a determination of the amount of time that a trade secret would have provided a commercial advantage or not be properly developed by a third party.[25]

Damages for both the actual loss suffered by the employer and any unjust enrichment enjoyed by the competitor as a result of the misappropriation may be awarded.[26] Specific performance may also be ordered to protect the compromised information.[27]

Punitive damages, in an amount not exceeding twice that awarded for actual damages and unjust enrichment, may also be awarded for willful and malicious misappropriation of a trade secret.[28]

The court may also award "the prevailing party reasonable attorneys fees and costs," and reasonable expert fees and costs, for willful misappropriation or for bad faith claims for damages or injunctive relief. "Bad faith" is defined as having been "undertaken or continued solely to harass or maliciously injure another, or to delay or prolong the resolution of the litigation, or that which is without any reasonable basis in fact or law and not capable of support by a good faith argument for an extension, modification or reversal of existing law."[29]

Claims and remedies under the NJTSA are likely cumulative, and do not pre-empt other claims.[30]

## The Defend Trade Secrets Act

On April 27, 2016, Congress passed the DTSA, which became effective on May 11, 2016, when it was signed into law by President Barack Obama.[31] It amended the Economic Espionage Act of 1996 (EEA) to include civil remedies in federal courts similar to those in the USTA and NJTSA.[32] "The DTSA undoubtedly provides trade secret owners with a new layer of protections in a world where trade secrets have become a company's lifeblood, and yet hacking and corporate espionage have become commonplace."[33]

*Jurisdiction Under the DTSA*

Under the DTSA, a federal court has jurisdiction over a claim of misappropriation of a trade secret used exclusively on an internal basis by the victim, or which is related to a product or service in the development stage, so long as the trade secret is related to a product that is intended for use in interstate or foreign commerce.[34]

The DTSA applies to conduct outside the United States if: "(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States." Therefore, a foreign corporation that sells a product in the United States that embodies a stolen trade secret can likely be sued in the United States if the misappropriation occurred here, regardless of where the product was manufactured. Moreover, foreign companies that do business in the United States may be able to be sued here if an act in furtherance of the offense was committed here.[35]

Thus, "a trade secret owner who experiences a cross-border theft will unquestionably be better off utilizing the broad discovery powers attendant to being in federal court and relying on the strong remedies afforded by the DTSA."[36]

*Defining a Trade Secret Under the DTSA*

The DTSA defines trade secret to include information "of any form, regardless of how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, and of any type, financial, business, scientific, technical, economic, or engineering information, so long as: 1) the information is actually secret, because it is neither known to, nor readily ascertainable by, another person who can obtain economic value from the disclosure or use of the information; 2) the owner has taken 'reasonable measures' to maintain the secrecy; and 3) independent economic value is derived from that secrecy."[37]

Although the DTSA does not define reasonable measures, reasonableness varies depending on the "particular field or industry, the value of the trade-secreted material and other economic factors. However, the more security measures that are instituted, the more likely a court will find those measures" to be 'reasonable.'[38] The protected information must also derive "independent economic value...from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information."[39]

Under the DTSA, like the NJTSA and the USTA, information can be a trade secret if not "generally known by" and

not "readily ascertainable" through proper means by "another person who can obtain economic value from the disclosure or use of the information."[40] The DTSA also provides that information "stored" only in an individual's memory can be the subject of a civil claim for theft of trade secrets. Proprietary information that can be reverse engineered with relative ease and expense may render the information readily ascertainable and, therefore, not eligible for trade secret protection.[41]

Thus, the key to qualifying as a trade secret is whether the competitors of the trade secret owner actually know or can easily discover the secret.[42] Every part of the information need not be completely confidential to qualify for protection as a trade secret. A trade secret can include a combination of elements that are in the public domain if the trade secret constitutes a unique "effective, successful and valuable integration of public domain elements."[43]

*What Constitutes Misappropriation Under the DTSA*

Misappropriation under the DTSA, like under the NJTSA and the USTA, occurs where a trade secret is acquired by a party who, without permission: 1) knowingly obtains the trade secret through improper means, or 2) discloses or uses a trade secret knowing either: 1) that it is a trade secret, or 2) that it was obtained through improper means.[44]

Improper means include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[45]

Disclosure or use means:

> a person—(i) used improper means to acquire knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—(I) Derived from or through a person who used improper means to acquire the trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or (iii) before a material change of the position of the person, knew or had reason to know that—(I) the trade secret was a trade secret; and (II) knowledge of the trade secret had been acquired by accident or mistake.[46]

Additionally, and like the UTSA and NJTSA, misappropriation does not include "reverse engineering, independent derivation, or any other lawful means of acquisition."[47]

*Non-Seizure Remedies Under the DTSA*

The DTSA also enables a party to obtain injunctive relief "to prevent any actual or threatened misappropriation," provided that it does not "(I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence or threatened misappropriation and not merely on the information the person knows; or (II) otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade or business."[48] The DTSA only allows injunctions "with respect to an employment relationship" where "there is evidence of threatened or actual misappropriation, 'not merely on the information the employee knows.'"[49]

"[E]xceptional circumstances that render an injunction inequitable" can condition the future use of the trade secret upon payment by the defendant of a reasonable royalty "for no longer than the period of time for which the use could have been prohibited."[50]

The DTSA allows a party to obtain actual damages, compensation on further offending parties' unjust enrichment "caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss;" or "in lieu of damages measured by any other methods." The damages caused by the misappropriation may be measured by imposition of liability for a reasonable royalty for the misappropriator's unauthorized disclosure or use of the trade secret.[51]

The court may also award "exemplary" damages of no more than two times the amount of actual damages awarded in the event the trade secret was "willfully and maliciously misappropriated."[52]

If a claim of the misappropriation is made in bad faith, "which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated [the court can] award reasonable attorney's fees to the prevailing party."[53]

The DTSA, like the NJTSA, does not preempt other claims.[54]

## Seizure Under the NJTSA and the DTSA

The NJTSA, like the UTSA, does not provide an explicit seizure remedy, but merely provides that "In appropriate circumstances, affirmative acts to protect a trade secret may be compelled by court order."[55] At least one court has found that such "affirmative acts" include seizure of allegedly misappropriated trade secret materials.[56]

The DTSA, unlike the NJTSA and the UST, expressly provides for seizure of stolen trade secrets, if significant prerequisites are met and procedures are followed.[57] Under the DTSA, a court can order the *ex parte*, civil seizure of property in "extraordinary circumstances" when "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[58]

There are eight mandatory requirements to obtain such a seizure order.[59]

1. The plaintiff must establish that an injunction or other available civil equitable remedy "would be inadequate" "because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order."
2. The trade secret owner must establish that it will suffer an "immediate and irreparable injury" if a seizure order is not granted. In most cases, this should not be an issue, because once a trade secret is disclosed it becomes largely valueless and the trade secret owner will suffer "irreparable injury," especially if the trade secret is on its way overseas, where the trade secret owner may have limited rights or remedies.[60]
3. The trade secret owner must show that the harm it will suffer absent seizure: 1) outweighs the harm to the "legitimate interests of the person against whom" the seizure is requested, and 2) "substantially outweighs the harm to any third parties" that might be caused by the seizure, who may, for example, have no knowledge that their new employee is bringing a stolen trade secret to the new job.[61]
4. The applicant must establish that it is likely to succeed in showing that the "information is a trade secret" and the person "misappropriated the trade secret of the applicant by improper means or conspired to use improper means to misappropriate the trade secret of the applicant."[62]
5. The trade secret owner must show that the person against whom the seizure is sought has possession of the trade secret and any property to be seized.[63]
6. The applicant must describe with "reasonable particularity" the property to be seized and the location of the trade secret to the extent reasonable under the circumstances.[64]
7. A trade secret owner must establish that the person against whom the seizure order is issued would "destroy, move, hide or otherwise make [the trade secret]...inaccessible to the court, if the applicant were to proceed on notice."[65]
8. A seizure order will not be issued if the trade secret owner has "publicized the requested seizure."[66]

Even if seizure is allowed, the seizure order must:

1. Set forth "findings of fact and conclusions of law required for the order;"[67]
2. Provide for the narrowest seizure necessary to accomplish the purpose;[68]
3. Direct the seizure to be undertaken in a manner that "minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;"[69]
4. Provide "guidance to law enforcement officials executing the seizure that clearly delineates the scope of the authority."[70]
5. Require a hearing no later than seven days after the seizure order has issued, where the applicant has "the burden to prove the facts supporting the findings of fact and conclusions of law necessary to support the order."[71] If the party fails to meet that burden, the seizure order shall be dissolved or modified appropriately. The order must also allow the party against whom the seizure order is directed to move to dissolve or modify the order;[72] and
6. Provide that the party seeking seizure provide security (as determined by the court) adequate for the payment of damages that may be suffered by virtue of a wrongful or excessive seizure.[73]

The DTSA also contains additional provisions to protect the party against whom the seizure is sought.

1. The court must "take appropriate action to protect the person against whom" the seizure was granted from publicity by the applicant about the seizure order.[74]
2. All seized materials "shall be taken into the custody of the court."[75]
3. If the "seized material includes a storage medium" or the trade secret is allegedly "stored on a storage medium, the court shall prohibit [it] from being connected to a network or the Internet without the consent of both parties, until the hearing is held."[76]
4. The court must "take appropriate measures to protect the confidentiality of seized materials that are unrelated to the trade secret information seized...unless the person against whom the order is entered consents to disclosure of the material."[77]
5. A "special master" may also be appointed to "locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized."[78]
6. The court may also permit a technical expert, "unaffiliated with the applicant...to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure."[79]
7. A copy of the seizure order must be served by the law enforcement officer effectuating the seizure, and the applicant cannot be involved in the seizure.[80]

The court may also modify the time limits for discovery under the Federal Rules of Civil Procedure, as may be necessary to facilitate the hearing, by permitting, for example, expedited discovery.[81]

Lastly, any person "claim[ing] an interest in the subject matter seized" may make a motion at any time seeking to encrypt the seized material and "[t]he motion shall include, when possible, the desired encryption method."[82]

The DTSA provides the person against whom the seizure was obtained with a cause of action "for wrongful or excessive seizure...and shall be entitled to the same relief as is provided under...15 U.S.C. sec. 1116(d)(11)."[83]

Thus, seizure under the NJTSA and DTSA requires an applicant to dive head first into uncharted waters. The DTSA provides an expressly defined right to seizure, but only if the applicant survives a gauntlet of significant prerequisites—and exposes the applicant to possible suit. In contrast, the NJTSA does not expressly provide for seizure, but arguably gives the court discretion to order seizure under appropriate circumstances in a more flexible, less burdensome fashion, and provides fee-shifting, but not a 'full-blown' cause of action, for wrongfully seeking seizure.[84] Moreover, New Jersey's state courts might now consider the DTSA's criteria when evaluating applications for seizure under the NJTSA.

Technical factors may also be consequential when parties seek seizure. For example, a person stealing a trade secret might email, or download to a flash drive, a substantial number of stolen electronic files. Obviously, the flash drive can be seized, but the seizure provision apparently allows seizure of every other copy of allegedly stolen information, which could include every computer that contains one or more stolen files, along with any hard copy files containing printouts. Read literally, every storage medium of a departing employee's new employer potentially would be subject to seizure. A thorough seizure in a departing employee situation could easily shut down the new employer until the hearing.[85]

In one recent pre-DTSA case, the trial court entered and later "reluctantly" dissolved a temporary restraining order, which had enabled the plaintiff to "seize, retain, and search" a defendant's computers and "scrub off its protected information, because of an inability to formulate an appropriate protocol for the review of the electronic material to isolate [plaintiff's] protected information at an expense which [plaintiff was] willing to bear," not because "the Seizure Order, and the procedures related thereto, lacked merit."[86]

Therefore, applicants for a seizure order should consult with information technology (IT) and cybersecurity experts, and provide the court with affordable mechanisms that "ally courts' concerns—and improve their odds of obtaining the order"[87]—based on the specific facts and technology in their case.

### Analysis and Practice Tips

Given the pace of technology, and "the bad guys of the world" who "continue to devise new and ingenious ways

of attempting to steal our clients' confidential information through cyberspace,"[88] businesses should take appropriate steps to protect their trade secrets. "Preventing dissemination [of a stolen trade secret] before it begins could make the difference between a merely unfortunate security breach and a disasterous one."[89]

Implementing reasonable measures to keep proprietary confidential information secret will not only protect them from misappropriation, taking such measures will also enable a court to treat the stolen information as a trade secret and to provide the victim with claims and remedies under the NJTSA and DTSA. Moreover, under the right circumstances, and particularly in the age of cyber theft, installing appropriate safeguards may enable a party to locate and seize its trade secrets, or at least enjoin the movement, disclosure and use of such information during the litigation.

*Keep Secrets Secret*

Courts require trade secret plaintiffs to protect their trade secrets, but do not generally require cost-prohibitive measures.[90] However,

> [a]s cloud computing, cognitive computers [etc.] expand, traditional elements of IP protection and enforcement will inevitably change. The definition of what constitutes "reasonable measures' to keep information confidential in trade secret law will shift as technology makes it easier for information to be hacked.[91]

Since the need for and sufficiency of these and other measures is as much a technological question as a legal one, businesses should regularly consult with IT security vendors as well as their lawyers to make sure their trade secrets are as secure as technology and economics will reasonably allow. However, some basic safeguards come to mind that are legally or practically required. For example, businesses should take the following measures:

- Have all employees sign agreements that stipulate that certain information is a trade secret and subject to trade secret protection; provide notices required by the DTSA of immunity for disclosure in certain situations,[92] and which otherwise limit the employee's right to disclose or use such information.
- Limit access to trade secrets to employees who need access to perform their jobs.
- Have their trade secrets subject to password protection.
- Have confidential information marked as confidential.
- Regularly remind and educate employees with access to confidential information about keeping such information secret.
- If feasible, segregate networks, or at least install firewalls, so hacking of one network, or one part of a network, does not expose information in the companies' other network or portion of a network.
- Engage outside specialists to monitor access and audit computer and electronic storage systems.[93]

*Enable Stolen Secrets to be Located*

"[P]rotective cybersecurity" "includes technological best practices," including "real-time analytics."[94] Additionally, while complete "retriev[al]" may be "almost impossible," "tracking devices" may be installed on certain electronically stored information that provide a "beacon home" to the owner that may help locate the stolen trade secret.[95] Although these beacons have limitations, in part because hacked information is often sent to various interim locations before reaching its final destination, beacons may help locate Microsoft and pdf documents.[96]

*Buy Time and Mitigate Damages*

The use or dissemination of a misappropriated trade secret may be limited, or at least delayed, if the stolen information is encrypted. Like a stolen safe that cannot be opened, trade secrets might not be used if they cannot be decoded. Therefore, encrypting trade secrets may prevent, or at least reduce, damage caused by the theft of a trade secret, and buy time to locate and seize stolen information before the thief cracks the code.

## Conclusion

The NJTSA and DTSA must still be sorted out in the courts, and are being applied to a high-tech moving target. Therefore, attorneys who represent businesses concerned about their trade secrets should regularly revisit these issues with their clients, preferably in consultation with cybersecurity companies.

***John A. Stone*** *is a partner with DeCotils, FitzPatrick & Cole, LLP. His practice includes commercial, intellectual property and construction litigation, including trade secret claims, in New Jersey and New York.*

ENDNOTES

1. Famous Cases of Espionage, www.bloomberg.com/news/photo-essays/2011-09-20 (July 28, 2016).
2. *Id.*
3. *See, e.g.*, Elizabeth A. Rowe, Rats, Traps, And Trade Secrets, 57 *Boston College Law Review* 301, 310 (March 2016)(*citing* 18 U.S.C. 1030(2)(c). ("In early February, 2013, a government report detailed the 'unrelenting campaign of cyberstealing linked to the Chinese government,'" including "hackers run by the Chinese People's Liberation Army"). Joel Brenner, The New Industrial Espionage, *The American Interest*, Winter (Jan./Feb. 2015), pgs. 29 and 31. (In 2010, Google disclosed that "Chinese cyberspies had penetrated its networks, stolen source code and used Google both to spy on its users and to worm their way into many other companies." The "level of cyber banditry, most of it from China has reached alarming levels.").
4. N.J.S.A. 56:15-1, *et seq.*
5. 18 U.S.C. 1836, *et seq.*
6. Other statutes that might, for the sake of argument, apply to cyber theft of trade secrets are not addressed in this article because the NJTSA (and the Uniform Trade Secrets Act on which the NJTSA is based) and the DTSA were specifically designed to provide civil relief in the way that other statutes were not. For example, the Computer Fraud and Abuse Act, 18 U.S.C. 1030, (CFAA) "was not enacted with trade secret protection in mind; it is an anti-hacking statute." *Big Rock Sports, LLC v. Acusport Corporation*, 2011 WL 4459189, n.1 (E.D.N.C. 2011), imposes criminal penalties for intentionally accessing a computer without authorization, or surpassing authorization. Rowe, *supra* note 6 at 310)(*citing* 18 U.S.C. 1030(2)(c). Additionally, "there are a variety of requirements in order to bring a claim under the CFAA, and it is often not applicable to common instances of trade secret misappropriation." Aaron Marks and Drew Hollander, Defend Trade Secrets Act: Planning Ahead And Strategic Choices, Corporate Counsel, www.corporatecounsel.com, pg. 2 (May 17, 2016). For example, in New Jersey, liability under the CFAA only exists where the offender's access to the information was not authorized, irrespective to the employee's motivation for accessing the information. Liability under the CFAA does not exist where the employee was authorized to access the information he later utilized to the possible detriment of his former employee. *Giraurdian Fragrances Corp. v. Krivda*, 2013 WL 5411475 (D.N.J. 2013) [citations omitted]. The Pre-DTSA Economic Espionage Act of 1996, 18 U.S.C. 1831-1839 (EEA) "provides for two distinct criminal trade secret offenses," one for "trade secret theft" and one for "foreign economic espionage." Mark L. Krotoski, Greta L. Burkholder, Jenny Harrison and Corey Houmand, the Landmark Defend Trade Secrets Act of 2016, Morgan Lewis White Paper, pg. 5, www.morganlewis.com (May 2016). The DTSA "amends the EEA to provide new civil remedies." *Id.*
7. Scott J. Shackelford, Symposium: Cyberwars: Navigating Responsibilities for the Public and Private Sector; Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk, 19 *Chap. L. Rev.* 445, 449 (Spring 2016).
8. Danielle K. Birdsong, Keeping the Best Kept Secrets: Mandatory Minimum Sentencing for Trade Secret Theft Under the Economic Espionage Act, 41 *New England Journal on Criminal and Civil Confinement* 421, 421-22 (Spring 2015); *See also*, Shackelford *supra* note 7 at 449 ("although some estimates count trade secrets losses as cybercrime, while others as espionage," the "G20 nations were estimated to have lost $200 billion to cyberattacks in 2014 alone"); John Villasenor, Corporate Cyber Security Realism: Managing Trade Secrets in a World Where Breaches Occur, 42 *AIPLA Q. J.* 329, 343 (Spring Summer 2015) ("It is beyond doubt" 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").
9. Birdsong, *supra* note 8 at 422.
10. Rowe, *supra* note 3 at 422-23.
11. Birdsong, *supra* note 8 at 426.
12. *Id.* at 426.
13. Rowe, *supra* note 3 at 382.
14. Birdsong, *supra* note 8 at 426.
15. Villasenor, *supra* note 8 at 343.
16. Bailey King and Whit Peirce, Creative Opportunities; The Defend Trade Secrets Act of 2016 is Here, and it's a Big Deal, 58 No. 7 *DRI For Def.* 42, pg. 1 (July 2016); Villasenor, *supra* note 8 at 337; Marks, *supra* note 6 at 2.
17. N.J.S.A. 56:15-2.
18. *Baxter v. Healthcare Corporation v. HQ Specialty Pharma Corporation*, ___ F.Supp. 3d ___ (D.N.J. 2016) (*citing* N.J.S.A. 56:15-2).
19. *Id.* (*citing* N.J.S.A. 56:15-2).
20. N.J.S.A. 56:15-2.
21. *Baxter v. Healthcare Corporation v. HQ Specialty Pharma Corporation*, ___ F.Supp. 3d ___ (D.N.J. 2016) (*citing* N.J.S.A. 56:15-2).
22. *Baxter v. Healthcare Corporation v. HQ Specialty Pharma Corporation*, ___ F.Supp. 3d ___ (D.N.J. 2016) (*citing* N.J.S.A. 56:15-2).
23. N.J.S.A. 56:15-3(a).
24. N.J.S.A. 56:15-3(b).
25. *See, e.g., Atlantic Inertial Systems, Inc. v. Condor Pacific Industries Of California, Inc.*, 2015 WL 3825318, *11 (C.D. Cal. 2015)(a royalty is, in effect, the price of a "suppositious license based upon the 'hypothetical' negotiations of the parties at the time the misappropriation

occurred" which, in turn, can be based on "fifteen factors" set forth in *Georgia Pacific Corp. v. U.S. Plywood Corp.*, 318 F.Supp. 1116, 1120 (S.D.N.Y. 1970), *modified sub nom, Georgia Pacific Corp. v. U.S. Plywood Champion Papers, Inc.*, 446 F.2d 295 (2d Cir. 1971)); *Linko, Inc. v. Fujitsu Ltd.*, 232 F.Supp. 2d 182, 186 n.7 (S.D.N.Y. 2002)("a jury should consider the following when determining a reasonable royalty: (1) the resulting and foreseeable changes in the parties competitive posture; (2) the prices, past purchases or licenses may have been paid; (3) the total value of the secret to the plaintiff, including the plaintiff's development costs and the importance of the secret to the plaintiff's business; (4) the nature and extent of the use the defendant intended for the secret,(5) whatever other unique factors in the particular case might have affected the parties' agreement, such as the ready availability of alternative process").

26. N.J.S.A. 56:15-4(a).
27. N.J.S.A. 56:15-3(c).
28. N.J.S.A. 56:15-4(b) and N.J.S.A. 56:15-6(a).
29. N.J.S.A. 56:15-6.
30. *SCS Healthcare Marketing, LLC v. Allergan USA, Inc.*, docket no. C-268-12 (Ch. Div. Bergen County 2012).
31. Peter J. Toren, 28 No. 7 *Intell. Prop. & Tech. L.J.* 3 (July 2016).
32. *Id.*; *See also*, Jonathan Eric Lewis, The Economic Espionage Act and the Threat of Chinese Espionage in the United States, 8 *Chi-Kent J. Intell. Prop.* 189, 191 (Spring 2009) (The EEA "was the first federal statute that provided criminal penalties for the misappropriation of trade secrets"). Without the DTSA amendment, the EEA "makes it a crime to steal and trade secrets for the economic benefit of anyone other than the owner...while intending on knowing that the offense will injure any owner of that trade secret." Peter J. Riebling, Landmark Trade Secrets Law Created New Federal Civil Cause of Action and Compliance Obligations for all Employers, 23 No. 3 *Westlaw Journal of Intellectual Property*, 2, pg. 1 (June 2, 2016)(*citing* 18 U.S.C. 1931).
33. Marks, *supra* note 6 at 1.
34. King, *supra* note 16 at 2.
35. *Id.* at 7.
36. Marks, *supra* at 3.
37. 18 U.S.C. 1839(3); Toren, *supra* note 31 at 5 (*citing United States v. Chung*, 659 F.3d. 815, 824-25 (9th Cir. 2011)); Krotoski, *supra* note 6 at 7.
38. Toren, *supra* note 31 at 3; Krotoski, *supra* note 6 at 14-15; *U.S. v. Hanjuan Jin*, 833 F.Supp. 2d 977, 1008 (N.D.Ill. 2013) ("Thus while a trade secret need not take 'every conceivable step to protect the property from misappropriation'" the "owner must employ precautionary measures that are reasonable under the circumstances"), *aff'd*, 733 F.3d. 718 (7th Cir. 2013).
39. 18 U.S.C. 1836(b)(2)(E); Toren, *supra* note 31 at 3; Krotoski, *supra* note 6 at 14-15; King, *supra* note 16 at 2.
40. Toren, *supra* note 31 at 2; King, *supra* note 16 at 2.
41. Toren, *supra* note 31 at 8-9; Krotoski, *supra* note 6 at 7; *See also*, John A. Stone, Reversal of Fortune: The Reverse Engineering Defense Under the NJTSA, 209 *N.J.L.J.* 920, S-8 (Sept. 17, 2012).
42. *Id.*; Krotoski, *supra* note 6 at 15.
43. Toren, *supra* note 31 at 3 (*citing Apollo Technologies v. Centrosphere Industries*, 805 F.Supp. 1157, 1197 (D.N.J. 1992)).
44. Toren, *supra* note 31 at 3-4.
45. *Id.* at 3; Krotoski, *supra* note 6 at 7.
46. 18 U.S.C. 1839(b)(5); Toren, *supra* note 31 at 3-4
47. 18 U.S.C. 1839(b)(6)(8); Toren, *supra* note 31 at 8-9.
48. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II).
49. 18 U.S.C. 1836(b)(3)(A)(I)-(II); Krotoski, *supra* note 6 at 11-12.
50. 18 U.S.C. 1836(b)(3)(A)(iii); Toren, *supra* note 31 at 6.
51. 18 U.S.C. 1836(b)(3)(A)(iii); Toren, *supra* note 31 at 6-7. Krotoski, *supra* note 6 at 7.
52. 18 U.S.C. 1836b)(3)(A)(iii); Toren, *supra* note 31 at 7; Krotoski, *supra* note 6 at 7; King, *supra* note 16 at 4.
53. King, *supra* note 16 at 3.
54. *Id.* at 2; Marks, *supra*, note 6 at 2.
55. N.J.S.A. 56:15-3c.
56. *Glycobiosciences, Inc.v. Woodfield Pharmaceutical, LLC*, 2016 WL 1702674, *1, *4 n. 5, and *10 (*citing* Section 134A.003(c) of the Texas Uniform Trade Secrets Act and Tex Civ. Prac. & Rem. Code Section 134A.003, which contain relevant language that is nearly identical to the wording of N.J.S.A. 56:15-3c and Section 2c of the USTA).
57. Anthony Stiegler, Watch Out: The Federal Trade Secrets Act Provides for *Ex Parte* Seizure, Inside Counsel www.insidecounsel.com (July 28, 2016); Krotoski, *supra* note 6 at 8-9.
58. 18 U.S.C. 1836 (b)(2)(A)(I); King, *supra* note 16 at 2; Toren, *supra* note 31 at 4-6 ; Krotoski, *supra* note 6 at 8-9. Courts may look for guidance to the seizure remedy in the Lanham Act, at 15 U.S.C. § 1116(d). However, the "types of fact inquires required for trade secret cases differ in important ways from the inquiries required in copyright and trademark cases; so although copyrights and trademarks have dedicated ex parte seizure provisions, the idiosyncratic attributes of trade secret cases make *ex parte* proceedings even more problematic." Eric Goldman, 72 *Washington & Lee L. Rev.* Online 284, 287 (Nov. 20, 2015).
59. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 4; Krotoski, *supra* note 6 at 8-9.
60. *Harry Schein, Inc. v. Cook*, 2016 WL 3418537 (N.D. Cal. 2016)(applying the DTSA and other law); *National Starch & Chem v. Parker Chem Corp.*, 219 N.J. Super. 158, 162 (App. Div. 1987)(applying pre-NJTSA law that is consistent with that statute); Krotoski, *supra* note 6 at 8-9 and 14.
61. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 4; Krotoski, *supra* note 6 at 8-9.
62. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 4; Krotoski, *supra* note 6 at 8-9.
63. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 4; Krotoski, *supra* note 6 at 8-9.
64. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.
65. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.
66. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.
67. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)

(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.

68. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

69. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(I)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

70. U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II). This provision was added to the DTSA to ensure that the extraordinary remedy of a seizure was accomplished in a manner that suits the circumstances of a particular case and protects both the victim and the party against whom the seizure is sought. The DTSA provides examples, including (i) the "hours during which the seizure may be executed," and (ii) "whether force may be used to access locked areas." Toren, *supra* note 31; Krotoski, *supra* note 6 at 8-9.

71. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.

72. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.

73. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5; Krotoski, *supra* note 6 at 8-9.

74. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

75. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

76. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

77. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

78. Toren, *supra* note 31 at 6 (*citing* 18 U.S.C. 1836(b)(2)(E); Bailey King and Whit Pierce, Creative Opportunities; The Defend Trade Secrets Act of 2016 is Here, and it's a Big Deal, 58 No. 7 *DRI for Def.* 42, pg. 3 (July 2016); Krotoski, supra note 6 at 8-9.

79. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(I)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

80. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 6; Krotoski, *supra* note 6 at 8-9.

81. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note; Krotoski, *supra* note 6 at 8-9.

82. 18 U.S.C. 1836(b)(3)(A(i)(I) and 1836(b)(3)(A)(i)(II); Toren, *supra* note 31 at 5-6; Krotoski, *supra* note 6 at 15.

83. Toren, *supra* note 31 at 5-6; Krotoski, *supra* note 6 at 8-9.

84. Stiegler, *supra* note 57.

85. *Clearone Communications, Inc. v. Bowers*, 509 Fed. Appx. 798, 800-01 (10th Cir. 2013).

86. Stiegler, *supra* note 57.

87. William M. Low, How One Firm Upgraded Security, 41 No. 4 *Litigation* 12 (Summer 2015).

88. Stiegler, *supra* note 57.

89. *American Center for Excellence In Surgical Assisting Inc. v. Community College Dist.*, 502, _____ F.Supp. 3rd ___, 2016 WL 316573, *6 (N.D. Ill. 2016) (whether steps taken to keep information confidential constitute a reasonable precaution under trade secret law depends on a balancing of costs and benefits that will vary from case to case"); *Xpertise, Inc. v. Cisco Systems, Inc.*, 2013 WL 867640, n.4 (D. Del 2013) (applying California law) ("courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets against flagrant industrial espionage"); *COI International, Inc. v. Merck*, 2005 WL 146890, *6 (E.D. Pa. 2005) ("Pennsylvania courts require relative (as opposed to absolute) secrecy to establish a trade secret and examine the precautions taken to protect a trade secret to ensure [they] are reasonable under the circumstances"); Rowe, *supra* note 3 at 310 (determining whether reasonable measures were used "necessarily calls for a cost-benefit analysis").

90. Goldman, *supra* note 58 at 290; *See also*, Howard C. Anawalt, IP Strategy: Complete Intellectual Property Planning, Access and Protection, Section 1:2 (July 2016 Update).

91. The DTSA "provid[es] immunity from claims of trade secret misappropriation to whistleblower employees who disclose their employer's trade secrets or confidential information to state or federal agencies for the purpose of reporting or investigating a suspected violation of law," which must be provided in all agreements with employees. Marks, *supra*, note 6 at 1. Failure to provide notice of this and other immunities provided by the DTSA to employees, consultants and independent contractors, in any contract or agreement entered into after May 11, 2016, that governs the use of trade secrets or other confidential information, "will strip the company of certain remedies (such as enhanced damages and attorneys fees) available in an action against an employee brought under the" DTSA. *Id.*; Susan Gross Sholinsky and Peter A. Steinmeyer, Strategies for Complying With Notice Provisions of Defend Trade Secrets Act of 2016, *National Law Review*, www.Natlawreview.com pg. 2 (2016). These notices, which employees would countersign, could, for example, state:

> Pursuant to the Defend Trade Secrets Act of 2016, I understand that:
>
> An individual may not be held criminally or civilly liable for any federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

*Id.* at 2. These required notices should be inserted in all: (i) employment, independent contractor and consulting agreements, (ii) separation, severance and release of claim agreements, (iii) non-compete and non-solicitation agreements, and (iv) confidentiality agreements and agreements in employee handbooks. *Id.*

92. Villasenor, *supra* note 8 at 346-355; Interview with Jason Rebholz, Director, The Crypsis Group (Aug. 29, 2016). For example, The Crypsis Group conducts "breach readiness reviews." www.crypsisgroup.com.

93. Shackelford, *supra* note 94.

94. Interview with Jason Rebholz, Director, The Crypsis Group (Aug. 29, 2016).

95. *Id.*; *See* www.crypsisgroup.com (describing a breach readiness review to help a client become "better prepared to self-detect and launch a rapid and effective response in the event of an incident").

96. Rebholz, *supra* note 95.