Implementing a Trade Secret Management Program

A Presentation for Trade Secret Management: Defining and Protecting Your Most Critical IP

October 10, 2024

Agenda

- What Constitutes a Trade Secret
- Trade Secrets are a Critical Asset Class
- The Power of a DTSA Enforcement Action
- Requirements for Bringing a DTSA Claim
- What Trade Secret Owners Can Do Now
  - Step 1: Identify and Classify
  - Step 2: Register and Secure
- Examples of Reasonable Measures (and What Are Not)

What Constitutes a Trade Secret?

What Constitutes a Trade Secret?

- The **Defend Trade Secrets Act** defines a "trade secret" as:
  - All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
    - (A) the owner has taken **reasonable measures** to keep such information secret; and
    - (B) the information derives **independent economic value**, actual or potential, 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.

What Constitutes a Trade Secret? (cont.)

- **What is "independent economic value"?**
  - Is the information used by the business or will it be?
  - Why does the information have independent economic value to the company or competitors?
  - What products or product lines does the information concern?
  - How much revenue is derived from the products or product lines?
  - How much does the revenue depend on the secrecy of the information?

Exemplary Trade Secret Categories

- Manufacturing process and protocols
- Raw data, extracted analytics, AI algorithms
- Software
- R&D, including failures (“negative know-how”)
- Customer and supplier information
- Information provided from customers
- Strategic, marketing and financial plans
- Analytical methods
- Testing data
- Quality specifications
- Stock/Inventory lists
- Materials lists
- Equipment (e.g., care and maintenance) information
- Training programs to ensure competency of required personnel
- Detailed descriptions of know-how and experience regarding errors to avoid, development and engineering process runs

Trade Secrets versus Patents

Every patent begins its life as a trade secret


The United States of America

The Director of the United States Patent and Trademark Office

Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

Therefore, this

United States Patent

Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, or importing into the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Michelle K. Lee

Director of the United States Patent and Trademark Office

Trade Secrets versus Patents (cont.)

Trade Secrets

- Confidential and internal
- No first-to-file issue – trade secret is valid and protectable from inception
- Any confidential information that confers a competitive advantage
- The existence of closely-related “prior art” does not invalidate a trade secret
- Public disclosure extinguishes trade secret
- No patent-eligibility issues

Patents

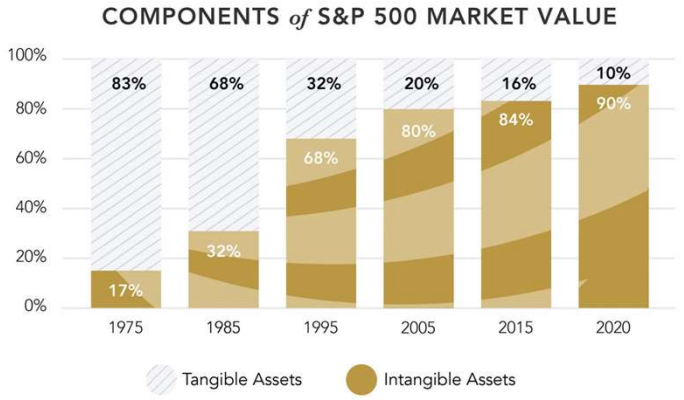
- Public disclosure of the claimed invention is required
- First-to-file gets to claim the invention
- Patentability determined by PTO
- Crowded field risks invalidation
- Patent eligibility, particularly with respect to software, is uncertain under the law
- The invention must be inventive and non-obvious but need not have independent commercial value

Trade Secrets are a Critical Asset Class

Trade Secrets are Critical Assets

- Intellectual property is a critical asset class
  - Patents, copyrights, trademarks are publicly disclosed and still protected; ***trade secrets*** are only secret until they're not
  - Over 35% companies surveyed say they have experienced a material IP event and most of these events relate to trade secrets at 41%

Source: https://www.aon.com/en/insights/articles/intellectual-property-an-asset-to-protect-and-leverage-in-the-technology



Source: https://oceantomo.com/intangible-asset-market-value-study/

- Companies should identify, manage and leverage all IP, **including their trade secrets**, to gain competitive edge, earn credibility with investors, and achieve higher valuation

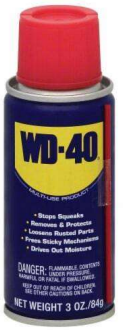
Trade Secrets are Critical Assets

- Trade secrets are the most vulnerable
  - Patents, copyrights and trademarks are government-registered and thus protected
  - ***Trade secrets are only secret until they're not***
    - "[M]ore than a third (35 percent) of the companies surveyed say they have experienced a material IP event. The majority of these IP events related to ***trade secrets (41 percent)***, with copyright issues at 26 percent."

Source: https://www.aon.com/en/insights/articles/intellectual-property-an-asset-to-protect-and-leverage-in-the-technologys

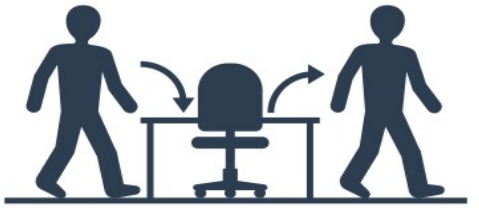
Trade Secrets are Critical Assets

- **Protecting Innovation**
  - Trade secrets are no less important than patents for protecting key technologies
  - Beyond the classic examples (Coca-Cola recipe and WD-40 formulation), there are millions of trade secrets driving innovation, competitive advantage and profitability
  - For early-stage companies, maintaining crown jewel assets as trade secrets can be a cost-effective alternative to patenting



Trade Secrets are Critical Assets

- **Protecting Innovation (cont.)**



  - Trade secrets are IP and must be protected as such
  - Mobility of key employees within the company and frequent job changes in many industry sectors make proactive protection of trade secrets essential
  - Trade secrets are increasingly becoming a target for theft
  - Not all companies are taking the necessary proactive steps to protect trade secrets until a key employee leaves the company. By then it is often be too late.

Trade Secrets are Critical Assets

- **Raising Capital and Improving Valuations**
  - Trade secrets are now a significant asset class in the IP portfolio – companies must identify, manage and leverage their trade secrets to impress investors

  - But companies often do not know what trade secrets they have and are not prepared to tell investors about them
  - Being able to articulate the importance of company trade secrets buys credibility and gives companies the ammunition for a higher valuation

The Power of a DTSA Enforcement Action to Protect Your Secrets

The Power of a DTSA Enforcement Action

- The DTSA, enacted in 2016, created a **federal private right of action** for trade secret misappropriation. Prior to the DTSA, trade secret owners could only pursue trade secret misappropriation claims under state trade secret laws.
- The DTSA provides many other benefits, including:
  - a federal cause of action that may pose less risk than patent litigation
  - protection for certain types of information that may not be well-suited for patent protection
  - an opportunity for claimants to secure large damage awards
  - allowing claimants to pursue trade misappropriation claims when the misappropriation largely occurred abroad

FORBES > TECH

The New 'Defend Trade Secrets Act' Is The Biggest IP Development In Years

Eric Goldman Former Contributor

I write about Internet law, intellectual property and advertising law

Apr 28, 2016, 01:04pm EDT

Yesterday, Congress passed the Defend Trade Secrets Act (the DTSA), which President Obama will sign soon. The Defend Trade Secrets Act extends the current Economic Espionage Act of 1996, which criminalizes certain trade secret misappropriations, to allow civil lawsuits. This gives trade secret owners a new and powerful option to bring trade secret lawsuits using federal law, whereas before only state law authorized their lawsuits. While creating a new federal trade secret claim to complement existing state law may sound more procedural than substantive, the DTSA actually has major consequences for intellectual property law and for our economy. This post highlights six implications.

Trade Secret Enforcement May Have Less Hurdles

- Patent litigation developments have encouraged companies to focus on trade secret protection

Patent Enforcement

- History of vacated damage awards at the Federal Circuit
- Successful challenges under 35 U.S.C. § 101 in U.S. district courts, limiting the types of innovations that are eligible for patent protection
- District courts frequently stay litigation pending validity challenges in front of the PTAB
- An increase in unfavorable IPR outcomes under 35 U.S.C. §§ 102 and 103 at the PTAB results in invalidated patents

vs.

Trade Secret Enforcement

- Lack of history of vacated damage awards
- Nothing analogous to 35 U.S.C. § 101 in the DTSA – no limit on the type of information that is eligible for trade secret protection.
- No PTAB or analogous administrative adjudication forum under the DTSA; DTSA claims are less likely to be stayed compared to a patent infringement claim.
- There is nothing analogous to 35 U.S.C. §§ 102 and 103 under the DTSA that would "invalidate" a trade secret claim

Some Innovations Are Better Protected as Trade Secrets

- Patents are not always the best mode of protection
  - Technology that may be aggressively challenged for not being eligible for patent protection under 35 U.S.C. § 101 (e.g., Google search algorithms, any **invention using artificial intelligence, customer lists**)
  - Technology that is technically a candidate for patent protection but nevertheless not easily litigated in courts (e.g., **manufacturing processes**)
  - **Information that is not easily reverse-engineered** and could be relevant for many decades (as patents have term limits) (e.g., recipes for a polymer solution)
- Trade secret protection under the DTSA is not dependent on the type of technology and has no term limit – a trade secret lives forever as long as it's a secret

The Potential for Large Damage Awards

- **A primary benefit of maintaining a trade secret inventory is to preserve value and competitive advantage**
- **A secondary benefit is the ability to recoup value through enforcement when trade secrets are misappropriated.**
  - The DTSA permits multiple types of damages under a single misappropriation claim. *Motorola Sols., Inc. v. Hytera Commc'ns Corp. Ltd.*, 2024 U.S. App. LEXIS 16120, *56-57 (7th Cir. 2024) (confirming **claimants can seek foreign sales** in addition to domestic sales)
  - The DTSA allows **both actual loss and unjust enrichment** damages. s*Medimpact Healthcare Sys. v. IQVIA Holdings Inc.*, 2022 U.S. Dist. LEXIS 186470, at *16 (S.D. Cal. 2022) ("An award of actual losses and unjust enrichment are permissible as long as there is no double counting.")
  - Claimants can get **punitive damages** and **attorneys' fees** if misappropriation is "willful and malicious," resulting ins large damage awards, e.g.:
    - *Comp. Sci. Corp. v. Tata Consultancy Servs. Ltd. et al.* (N.D. Texs.): In 2023, a jury awarded $210 million to the plaintiff (including $140 million in punitive damages).
    - *Resman, LLC v. Karya Prop. Mgmt. LLC* (E.D. Tex.): In 2021, a jury awarded $152 million to the plaintiff (including $90 million in punitive damages). The court's final judgment awarded $62 million.

Broad Extraterritorial Enforcement

- The DTSA **can be used to address trade secret misappropriation where the misappropriation occurred outside of the United States**

  DTSA applies to conduct occurring outside of the United States if the offender (1) is a citizen or permanent resident of the United States, (2) is a United States corporation, or (3) if "**an act in furtherance of the offense was committed in the United States**."

  See 18 U.S.C. § 1837

- The 7th Circuit recently confirmed the broad extraterritorial reach of the DTSA:

  *an act in furtherance of a civil misappropriation need not itself be a complete violation of the law. . . **[s]o long as "an act in furtherance of the offense was committed in the United States,"** 18 U.S.C. § 1837(2), **then all damages caused by the offense are recoverable** under sections 1836(b) and 1837(2), **wherever in the world the rest of the underlying conduct occurred.***

  See Motorola Sols., 2024 U.S. App. LEXIS 16120, at *50-51.

Requirements for Bringing a DTSA Claim

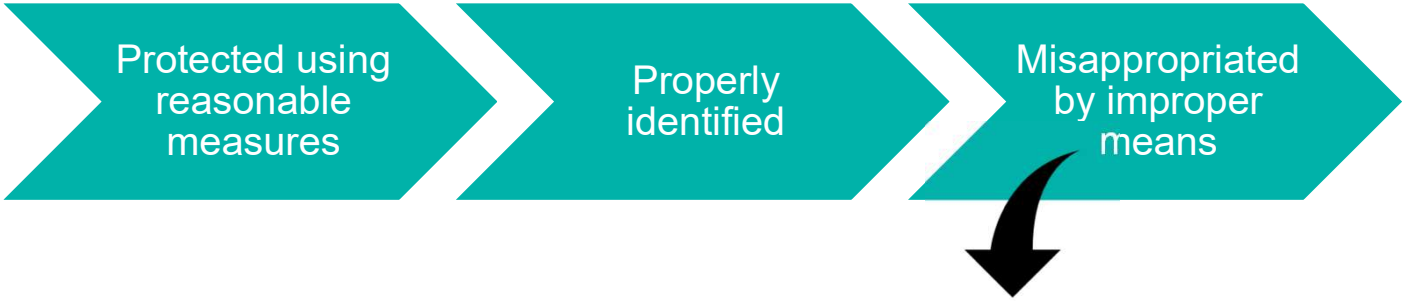
Requirements for Bringing a DTSA Claim

- *InteliClear LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653 (9th Cir. 2020):
  - "The Plaintiff 'should describe the subject matter of the trade secret **with sufficient particularity to separate it from matters of general knowledge in the trade.**"
  - "Plaintiffs **may not simply rely upon 'catchall' phrases or identify categories of trade secrets** they intend to pursue at trial."
  - "It is inadequate for plaintiffs to cite and incorporate by reference hundreds of documents that purportedly reference or reflect the trade secret information."
- *Insulet Corp. v. EOFlow Co., Ltd.*, No. 2024-1137 (Fed Cir Jun. 17, 2024):
  - Fed Circ reversed District Court decision stating that DC's definition of a trade secret was too broad.

Requirements for Bringing a DTSA Claim

- Mark documents as trade secrets
- Require confidentiality and nondisclosure agreements
- Establish policies for handling confidential information
- Restrict access
- Conduct employee training
- Audit and inspect regularly
- Exercise post-employment contractual obligations

Requirements for Bringing a DTSA Claim



Theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means

Note: the DTSA has a **Statute of Limitations** – three (3) years from when the misappropriation was discovered using reasonable diligence; thus, if you discover misappropriation, do not sit around and do nothings! *See, e.g., CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 920 F.3d 560 (8th Cir. 2019).

What Trade Secret Owners Can Do Now

How Trade Secret Owners Forfeit Their Rights

- Trade secret owners lose their rights by not sufficiently ***identifying*** and ***registering*** their secrets and/or protecting them using ***reasonable measures***:
  - **No Trade Secret Program**
    - absent trade secret protection, including contractual obligations, unpatented business information can be legally copied, disclosed, and used by anyone, including ex-employees, contractors, consultants, vendors and competitors
  - **Lack of Reasonable Measures**
    - failure to take reasonable measures to maintain the secrecy of information is the most common way to forfeit trade secret rights
    - courts require "reasonable measures" **before a trade secret is stolen**
  - **Inadvertent Disclosure Due to Lack of Identification**
    - due to a failure to identify trade secrets, employees inadvertently disclose trade secrets to the public during trade shows, conferences, sales calls, customer visits, FDA submissions, etc.

Step 1: Identify and Classify

- Establish a process to identify trade secrets and create an inventory—

(1) Generate a list of ***potential*** trade secrets;

(2) Categorize that list of ***potential*** trade secrets;

(3) Identify **actual** secrets from the list of ***potential*** ones; and

(4) Classify the **actual** trade secrets.

Step 1: Identify and Classify

(1) Generate a List of Potential Secrets

- This can be difficult as information assets are seldom physical—a trade secret portfolio is an amorphous and intangible cloud of information, stored on paper, in computer drives and in the minds of employees
- **EMPLOYEES ARE KEY** – information used in the normal course of business that derives value from being secret will be used and known by your employees
- ***BUT*** employees often do not know what qualifies as a "trade secret"

Step 1: Identify and Classify

(1) Generate a List of Potential Secrets (cont.)

- Four Steps:

(1) **Identify** relevant business units/engineering teams

(2) **Educate** employees so they can distinguish trade secrets from other information

(3) **Interview and collect** from key employees:

- potential trade secrets that they created or use in their job
- documents needed to prove the existence, ownership and value of each potential secret (e.g., lab notebooks, specifications, schematics)

(4) **Reconcile** the lists and remove redundancies

Step 1: Identify and Classify

(2) Categorize the List of Potential Trade Secrets

- Trade secrets often nicely fall into a categorization system of **"<Subject><Format> for <Product>"**
  - "**Subject**": department that created or uses the trade secret
  - "**Format**": document formats, prototypes, processes, formulas, results, plans and other categories that are appropriate for the company
  - "**Product**": usually the name or groups of products, e.g., a trade secret that applies to the bottling method for all carbonated beverages.
- ***Examples***: "Manufacturing Process for Disk Drives"; "Sales Forecast for Lawn Furniture"; "Engineering Specification for Transmission"

Step 1: Identify and Classify

(3) Identify *Actual* Trade Secrets

- Six (6) factors for identifying "actual" trade secrets*

(1) The extent to which the information is known outside the company

(2) The extent to which the information is known by employees

(3) The extent of measures taken to keep the information secret

(4) The value of the information to the company and competitors

(5) The amount of effort or money expended in developing the information

(6) The ease or difficulty with which the information could be acquired or duplicated

rate each factor on a scale of 1 to 5

Step 1: Identify and Classify

(4) Classify the Trade Secrets

- Trade secrets must be classified to indicate their sensitivity and guide their handling and security levels
  - E.g., while the structure of a sales incentive program may be confidential, it is likely not of the same sensitivity as the recipe for a flagship product
- A classification scheme should have 3 to 5 levels, including "**Not Confidential**" for general information and "**Personal Information**" for employee addresses, telephone numbers, etc.
- For **trade secret level(s)**, a "**Confidential and Proprietary**" level or a 3-tiered scheme of "**Confidential**," "**Secret**" and "**Top Secret**" are most common

Step 2: Register and Protect

(1) Internal Registration

- **Create a Trade Secret Registration Process and Registry**
  - Implement protocols and databases recording the trade secrets identified through the Inventory and Classification process
  - each document/file should be marked with an appropriate confidentiality designation
  - trade secrets can be organized by department on a secure network or on specific non-networked computers at a station or in a building accessible only to a discrete employees
  - weekly or monthly meetings with division heads/key personnel regarding new proprietary information/process
  - can be managed in-house or in collaboration with outside counsel

Step 2: Register and Protect

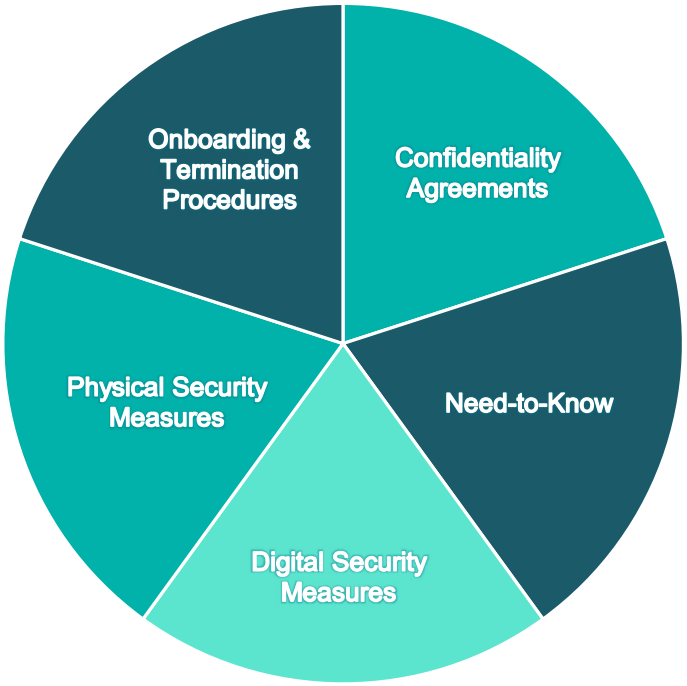
(1) Internal Registration (cont.)

– Five Elements of the Company Registry

- **Taxonomy** – trade secrets must be categorized into an easily-understood taxonomy, not a blob of undifferentiated knowledge
- **Scoring** – all trade secrets are not created equal; each trade secret must be scored using a scoring method that reflects legal standards and is easy to use
- **Metadata** – the trade secret itself should not be registered (only metadata about the secret)
- **History** – retain all versions of such metadata and be able to produce it as it existed at any prior time
- **Proof** – be able to prove that historical data is accurate and contemporaneous to a period of interest

Step 2: Register and Protect

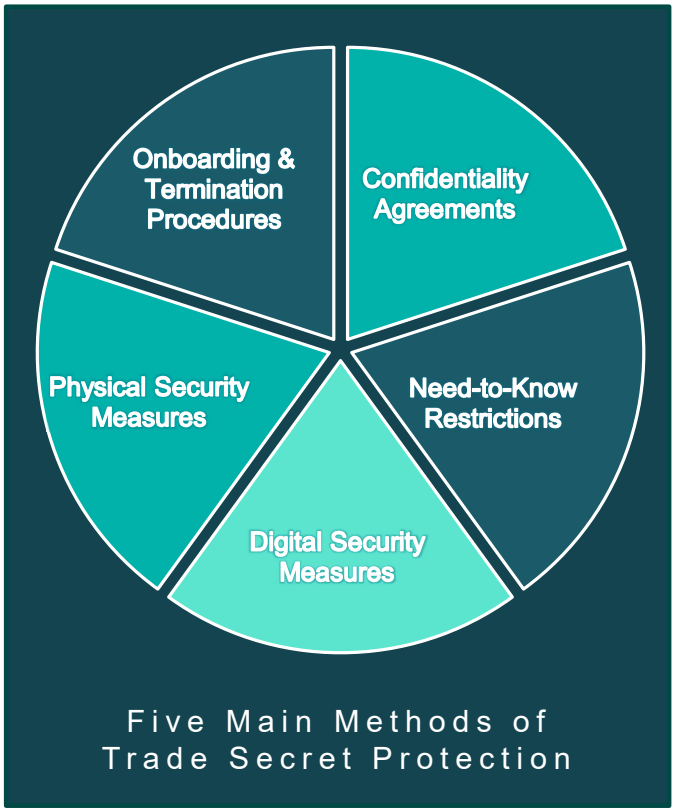
Reasonable Measures of Protection



Step 2: Register and Protect

Reasonable Measures – How It's Done

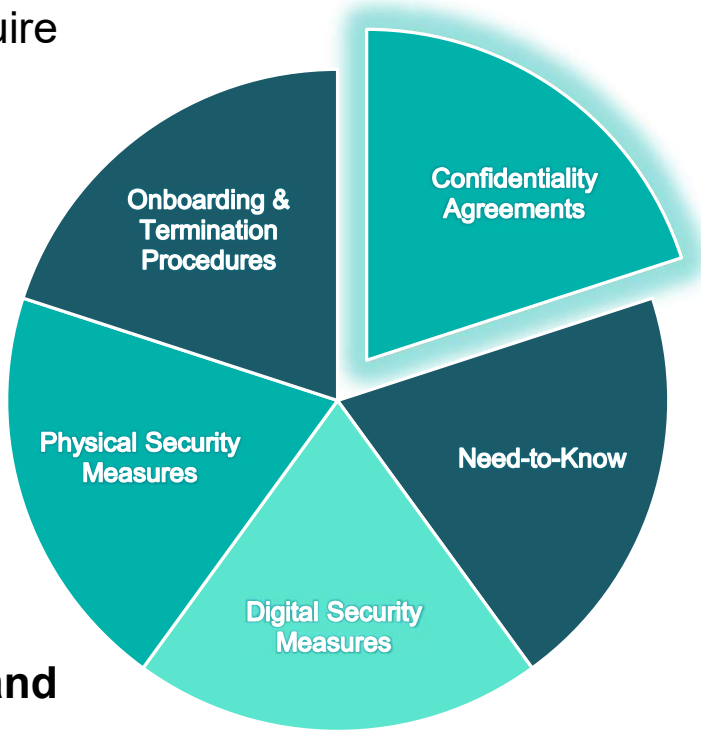
- After identifying potential trade secrets:
  - Identify current protections
  - Implement a risk assessment to determine whether a trade secret is susceptible to secrecy breaches
  - Identify additional protections from the **five main methods of trade secret protection** based on the types of risks identified
  - Select additional protections by balancing the practical and legal need for protection and the cost of the protection



Step 2: Register and Protect

Confidentiality Agreements

- Identify parties with access to trade secrets and require confidentiality agreements **before exposing trade secrets**
- Parties with access may include:
  - Employees with access
  - Auditors
  - Customers
  - Out-sourced production or testing
  - Contractors
  - Cloud-based document repositories
- **Periodically review and audit** confidentiality agreements
- The confidentiality agreements need to be in **written form and signed** (oral agreements likely do not suffice)



Step 2: Register and Protect

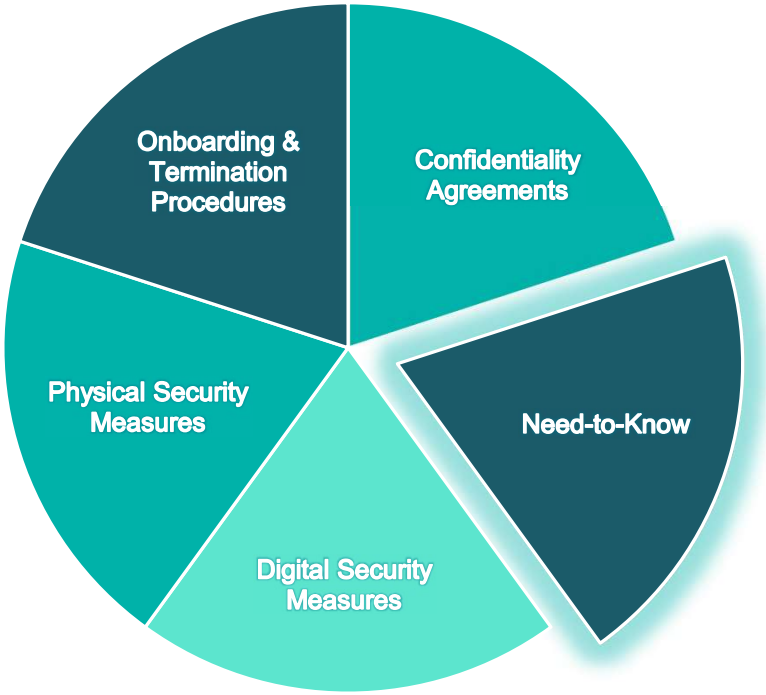
Confidentiality Agreements are Important

- While confidentiality agreements are not required, **courts find a lack of "reasonable measures" when trade secret owners do not use such agreements, even with other measures in place**
  - *DePuy Synthes Prods. v. Veterinary Orthopedic Implants, Inc.,* 990 F.3d 1364, 1371-72 (Fed. Cir. 2021) (affirming that trade secret owner did not demonstrate "reasonable efforts to maintain secrecy" irrespective of owner's other internal protective efforts because the trade secret owner failed to present evidence of a confidentiality agreement)
  - *Inv. Sci., LLC v. Oath Holdings Inc.,* 2021 U.S. Dist. LEXIS 151076, at *7-8 (S.D.N.Y. 2021) (finding lack of reasonable measures because secret was shared before defendant signed confidentiality agreement)
  - *Mason v. Amtrust Fin. Sen's.. Inc.*, 848 F. App'x 447, 450 (2d Cir. 2021) (affirming district court's finding of no reasonable measures because plaintiff "did not legally protect s[his] property by executing a nondisclosure or licensing agreement")

Step 2: Register and Protect

"Need-to-Know" Access

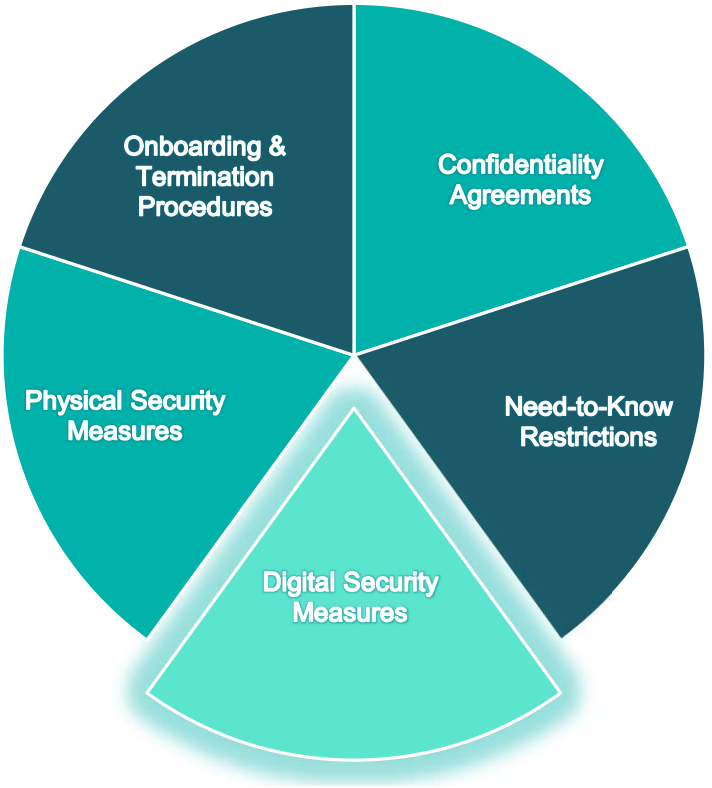
- **Limit access to facility areas** based on job function
- **Limit access to documents/repositories** based on job function
- **Only share product information** with customers **for the products** they purchases
- **Do not share information or samples** with third-parties (customers, auditors, contractors) **that is not covered by an NDA** or confidentiality agreement
- **Require an escort** for all visiting third-parties



Step 2: Registration and Security

Digital Security Measures

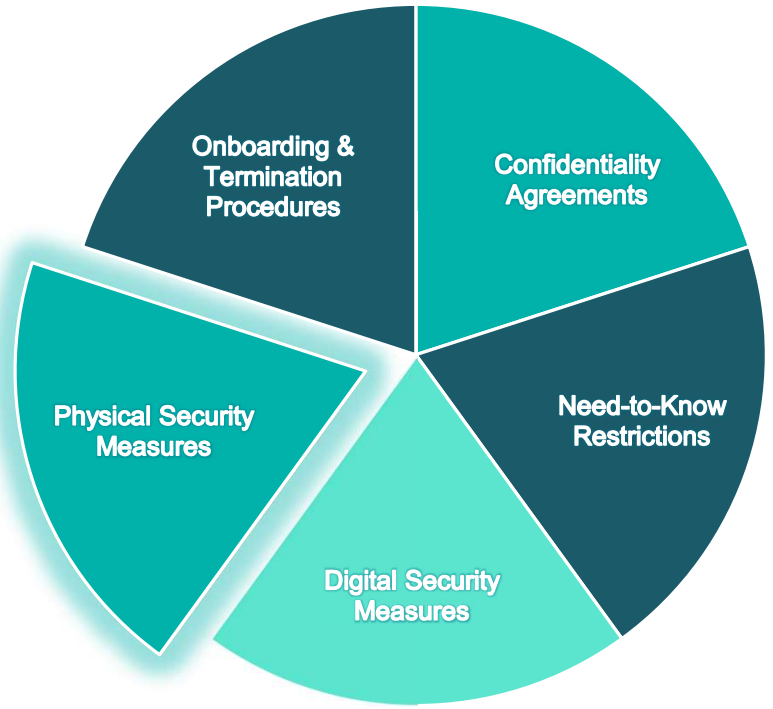
- **Implement authentication protocols on all computer terminals**
- **Limit access to document folders** using authentication procedures
- Create and implement company **email retention policy** (e.g., emails < 3 months old are archived and deleted from individual saccounts)
- Use **“proprietary”** or **“trade secret” labels** on all applicable documents
- Use **encryption** to protect in-transit and stored data (e.g., all cloud-based services should encrypt stored data)
- Implement **activity monitoring** (monitoring employees’ emails, downloads, and print jobs)
- Implement different levels of **firewalls** on computer terminals
- **Prohibit accessing** trade secrets **via personal devices**



Step 2: Register and Protect

Physical Security Measures

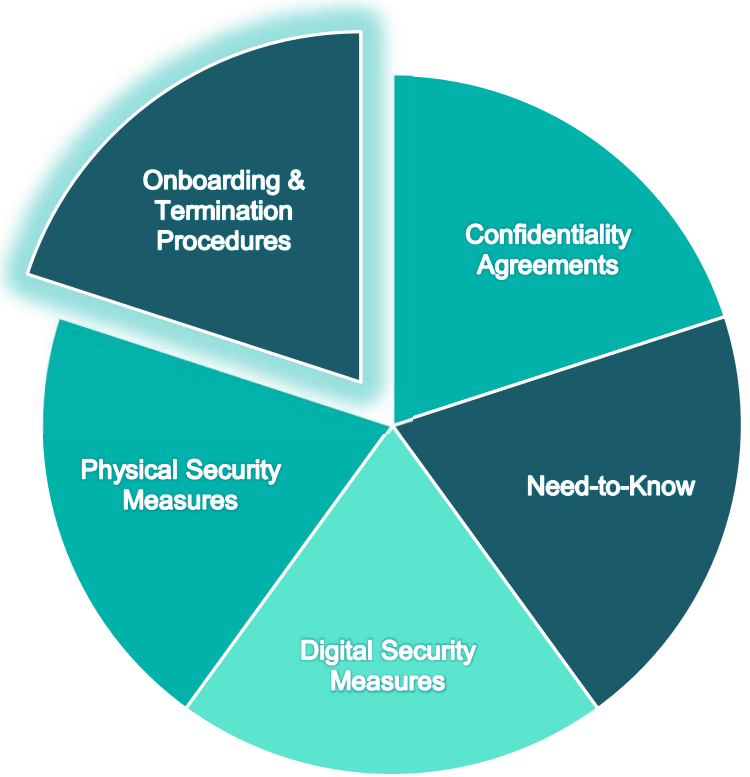
- **Limit accessibility to research and production areas** containing trade secrets using badges, passcodes, etc.
- **Limit viewership of research and production areas** containing trade secrets by
  - strategic placement of trade secrets in the facility (e.g., not in plain view)
  - install frosted windows
  - segregating work areas containing trade secrets from other work areas
- **Securely storing notebooks or papers** containing trade secrets at the end of each shift



Step 2: Register and Protect

Onboard & Termination Procedures

- Mandatory reading and signage of **employee handbook**
- **Regularly scheduled trainings** on company policies related to confidentiality and trade secrets
  - Including written confirmation of employees' attendance
- **Termination Protocolss**:
  - Requiring departing employees to return all laptops, USB drives, and company documents
  - Revoking an employee's access to digital accounts, including cloud storage accounts and company emails
  - Exit interviews to ensure all termination protocols and confidentiality protocols have been adhered to



Examples of Reasonable Measures

“Reasonable Measures” – Manufacturing

- Although often highly valuable, **manufacturing know-how can be difficult to protect using patents and may be best protected as trade secrets**
- Exemplary manufacturing trade secrets:
  - Process parameters (e.g. temperature, pressure, humidity, distance metrics)
  - Design capacities for a continuous and autonomous production line
  - Design of custom-made manufacturing equipment
  - Operator handling procedures for hazardous materials
  - Algorithms, PLC code, and proprietary software
  - Recipes (e.g., raw material amounts, sequence and conditions when adding raw materials)
  - Material specifications (e.g., polymer molecular weight or water content of solvent)

“Reasonable Measures” – Manufacturing

- Persons with access to the manufacturing floor must have confidentiality obligations, including equipment vendors, auditors, and customers
- Employee training
- Visitors must be accompanied by experienced company representatives that know how to handle customers asking for WIP samples, process specifications or other proprietary information
- Access to electronic repositories or other systems, such as MES systems, should be limited by location and to employees on a need-to-know basis
- Using personal devices on the production floor must be limited based on job function
- Hardcopies of production logs are stored in a secure place when not in use

“Reasonable Measures”s – Manufacturing: Case Study #1

- **Scenario**:
  - A customer tours the production facility of Company A and requests proprietary process documents from a technician. The technician provides the documents to the customer to make the customer happy and the customer gives the information to a competitor of Company A.
- **“Reasonable Measures” that Could Have Been Taken**:
  - All persons, including the customer representative, should have been under some form of NDA
  - The technician should have undergone training to better understand that the documentation contained secrets and how to employ tactics to protect information from third parties, e.g., referring the customer representative to the floor supervisor
  - A company representative tasked with mitigating such a request should have been present to explain that the company does not share the process documentation
  - The process documentation hardcopy should have been labeled as containing trade secret information

“Reasonable Measures” – Manufacturing: Case Study #2

- **Scenario**:
  - Company A contracts an equipment vendor to build and install custom manufacturing equipment to improve cycle time, including developing PLC code. The vendor later sells and installs the same equipment for a competitor of Company A who is also updating its manufacturing process.
- **“Reasonable Measures” that Could Have Been Taken**:
  - The vendor should have signed a robust NDA that assigned all right, title and interest in the intellectual property relating to the customer equipment to Company A and that prevented the vendor from sharing any information relating to its project with Company A
  - The vendor should have been required to handover all work product, including blueprints and PLC code, to Company As
  - The NDA should have required the vendor to include the same confidentiality provisions in its agreements with subcontractors

“Reasonable Measures” – Manufacturing: Case Study #3

- **Scenario**:
  - A manufacturing technician of Company A takes pictures of HMI screens and process specifications containing trade secrets with his personal cellphone and departs Company A for a similar manufacturing role at Company B down the street.
- **Reasonable Measures that Could Have Been Taken**:
  - The technician should have signed a written NDA
  - The technician should have undergone training to help him understand that the screens and specifications contain trade secrets and the legal ramifications of taking such information with him
  - The process documentation and HMI screen should have been labeled as containing trade secrets
  - The company should have conducting an employee exit interview to assess whether the technician has in his possession any company secrets and remind the technician of his confidentiality obligations
  - The company should include a policy that forbids usage of personal electronic devices on the production floor, tailored to job-function (supervisors often need cellphones, but technicians often do not)

“Reasonable Measures” – R&D

- Classify R&D outcomes as candidates for trade secret protection verses patent protection
- Review FDA submissions to ensure no inadvertent disclosure of secrets or that secrets are labeled appropriately
- Review all draft publications, including patent specifications, to ensure no inadvertent disclosure
- Joint development agreements with non-disclosure clauses and that identify who owns technology outcomes
- Secure storage of current and past research notebooks
- Limited access to R&D areas and repositories on a need-to-know basis

“Reasonable Measures” – Customer Lists

- In *Allstate Ins. Co. v. Fougere*, 79 F.4th 172, 192-93 (1st Cir. 2023), the Court found the trade secret owner took reasonable measures to protect its customer lists, including:
  - Only allowing specific employees (agents) to access the book of business
  - Password protecting books of business
  - Revoking the agent’s access to books of business upon agent termination information
  - Requiring confidentiality agreements between agents and Allstate
- Other protections that could have been implemented:
  - Requiring exit interviews with agents to ensure agents did not take books of business
  - Reviewing recent download and email history of departing agents

“Reasonable Measures” – Softwares

- In software cases, courts frequently look to:
  - who is given access to the software;
  - confidentiality agreements for all entities given access to software; and
  - whether source code was encrypted or compiled

See, e.g., *Turret Labs USA, Inc. v. CargoSprint*; *Inteliclear, LLC v. ETC Global Holdings, Inc.*, 978 F.3d 653, 660-661 (9th Cir. 2020)

Lack of Reasonable Measures

Lack of "Reasonable Measures"

- While perfection is not required, courts have identified circumstances that are ***not*** "reasonable measures" under the DTSA:
  - In *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888 (N.D. Ill. 2019), the owner did not:
    - require **confidentiality and nondisclosure agreements;**
    - **implement policies** concerning confidential business information;
    - **train employees** regarding confidentiality obligations;
    - **restrict access** to the information on a need-to-know basis; and
    - **take actions** to maintain the secrecy of information **when employees departed** the company.

Lack of “Reasonable Measures”

- In *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279, 1299-1300 (11th Cir. 2018), the trade secret owner:
  - **encouraged employees to store information on a personal laptop** and phone;
  - **did not require the defendant to sign the employment agreement** requiring employees to maintain company trade secrets;
  - **did not mark** the information as confidential; and
  - **did not require the defendant to delete the information** whens he left the company.

Lack of “Reasonable Measures” (cont.)

- In *RV Horizons, Inc. v. Smith*, No. 18-CV-02780-NYW, 2020 WL 6701119, at *26 (D. Colo. Nov. 13, 2020), the trade secret owner:
  - **did not limit access** to the software containing the trade secrets to specific individuals;
  - **did not separate the software** containing trade secrets from materials that were not trade secrets;
  - **did not inform the defendants** that information contained trade secrets; and
  - **did not provide confidentiality agreements, handbooks, or training**, regarding the confidentiality of the trade secrets.

Recent and Expected Trade Secret Law

Recent and Expected Trade Secret Law

- Recent Developments
  - Identifying trade secrets with sufficient particularity (See *InteliClear LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653 (9th Cir. 2020) and *Insulet Corp. v. EOFlow Co., Ltd.*, No. 2024-1137 (Fed Cir Jun. 17, 2024)
  - Extraterritorial reach and foreign sales (*See Motorola* (7th Cir. July 2024)).
- Future Developments
  - Implications of cloud computing and artificial intelligence in trade secret protection
  - Whether a defendant may present evidence of improving reasonable measures after misappropriation has occurred as proof reasonable measures were not implemented at time of misappropriation (this has not yet been litigated)

s