The six stages of trade secret protection

Mike Kasdan
David Cohen
Donal O'Connell

Celesq Webinar

November 18, 2020

About the presenters

Mike Kasdan

Michael Kasdan is the head of Wiggin and Dana's Trade Secret Practice Group. He has authored numerous articles on trade secrets and regularly speaks to clients about trades secret asset

David Cohen

David Cohen has been practicing IP law for over 20 years. He is the former Chief Legal and IP Officer at Vringo; Senior Counsel at Nokia; and was an IP lawyer first at Skadden Arps and then at Lerner David.

Donal O'Connell

Donal O'Connell is ex VP of R&D and ex Director of IP at Nokia; He has written over 80 short papers on trade secrets. His company has designed and developed both a trade secret audit tool as well as trade secret asset management solution.

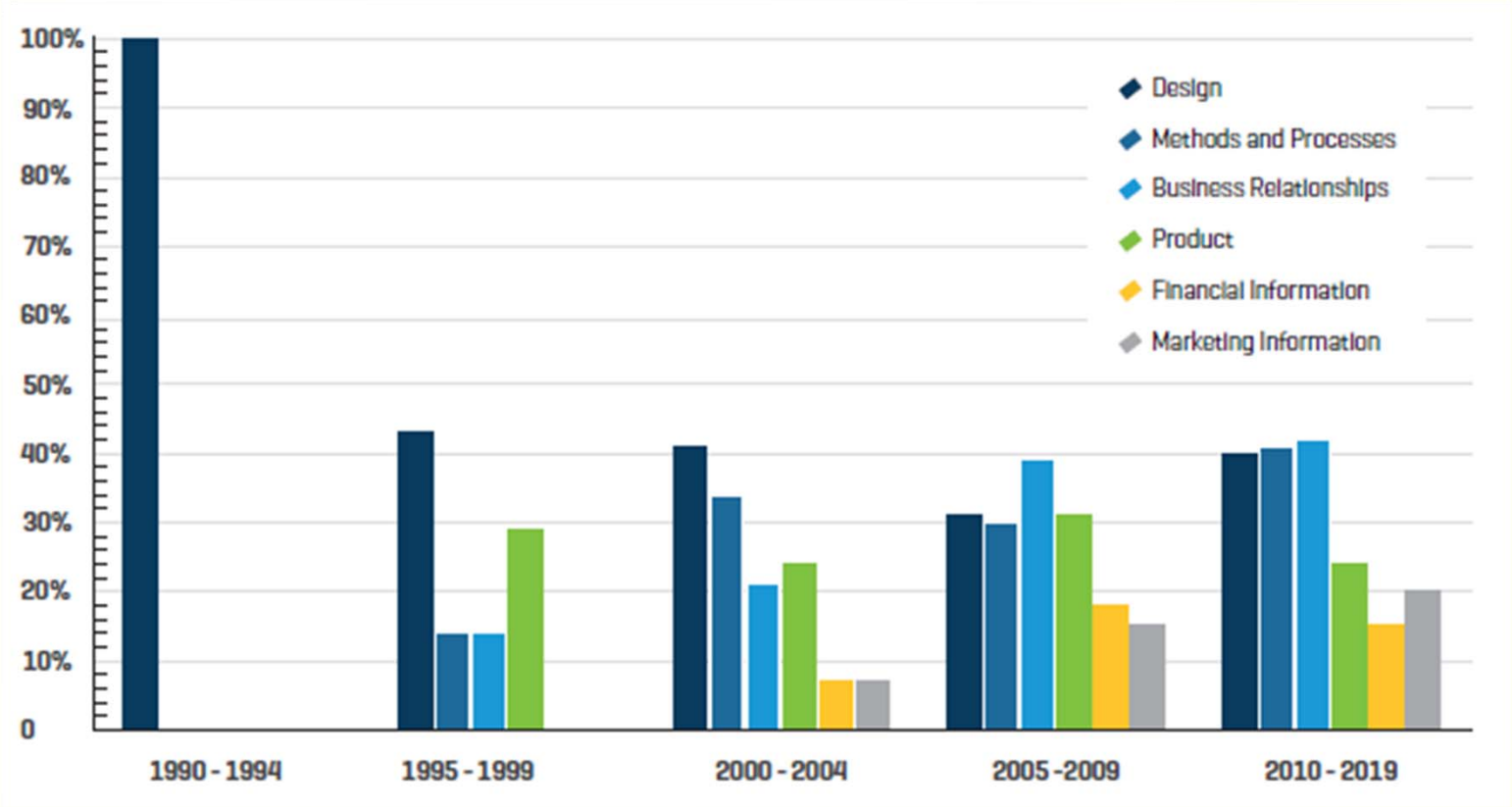
Trade Secret Basics

- Trade secrets - a creature of national law
  - Many countries didn't have a separate trade secret law
  - Historically trade secrets were treated as a kind of business tort (e.g. a wrongful act or an infringement of a right other than under contract)
  - Trade secrets being treated as IP is well established in some places, but quite novel in other places
- International and transnational agreements that limit how national governments can regulate trade secrets
  - EU Trade Secret Directive
  - Global tax treaties (e.g., OECD BEPS)
  - Global trade agreements (e.g. TRIPS)
- Implications
  - Differing remedies; enforcement mechanisms; litigation processes and protections; valuation processes, etc.

US IP laws – quick comparison

	Trade Secret (18 U.S.C. & state law)	Patent (35 U.S.C.)	Copyright (17 U.S.C. & state law)	Trademark (15 U.S.C. & state law)
Validity	secrecy (not generally known or available), value due to secrecy, reasonable efforts	novel, nonobvious, useful, adequately disclosed; *no abstract ideas or laws of nature*	independent creation, modicum of creativity, fixation; *no ideas, facts, or useful articles*	source-identifying, inherent/acquired distinctiveness, priority of use; *no generic words or functional features*
Infringement	acquisition by improper means or violation of confidential relationship	all-elements rule (or equivalents); making, using, offering to sell, selling, importing	actual copying & substantial similarity (copying, derivatives, distribution, performance/display)	likelihood of confusion or dilution due to defendant's use as a mark in commerce
Limitations	independent discovery, reverse engineering	experimental use, inequitable conduct, first sale	fair use, independent creation, first sale	abandonment, descriptive or nominative fair use, first sale
Remedies	*eBay* provides framework for evaluating whether injunction is appropriate; damages also available (including statutory damages for registered copyrights); potential criminal liability in all but patent			

Types of trade secrets in US litigation



Source: Trends in Trade Secret Litigation Report 2020, Stout

US trade secret definitions compared

Uniform Trade Secret Act (adopted in some form by all US states except New York)

§1(4) "Trade secret" means information … that:

(i) derives independent economic value … from not being generally known to, and not being readily ascertainable by proper means by, other persons…and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Federal Defend Trade Secret Act amendments to the Economic Espionage Act (18 U.S.C. § 1839(3))

§ 2(b)(1) the term "trade secret" means 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—

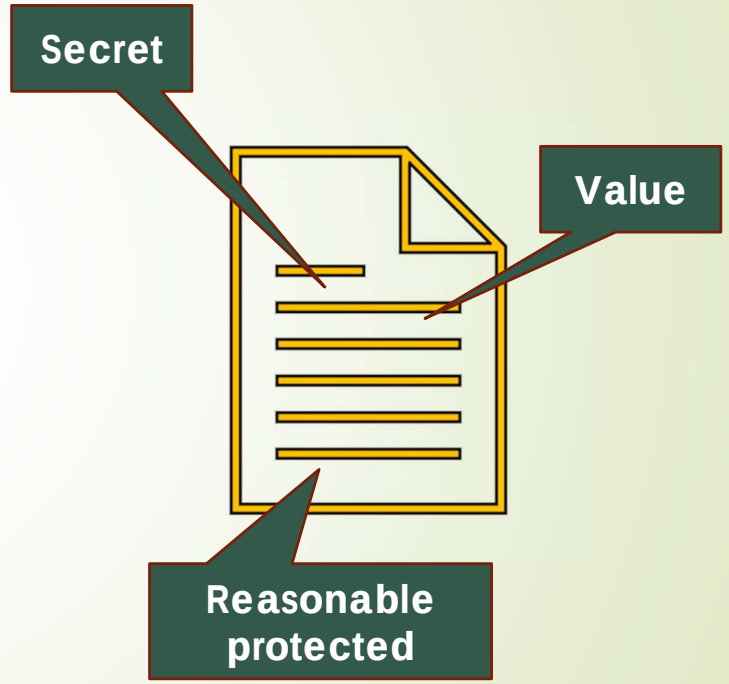
(A) the owner thereof has taken reasonable measures to keep such information secret; and

(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;

USTA's scope is broader; no limitations on the kind of "information" that can qualify
DTSA places the burden of "reasonable" measures or efforts on owner

Trade secrets - Summary

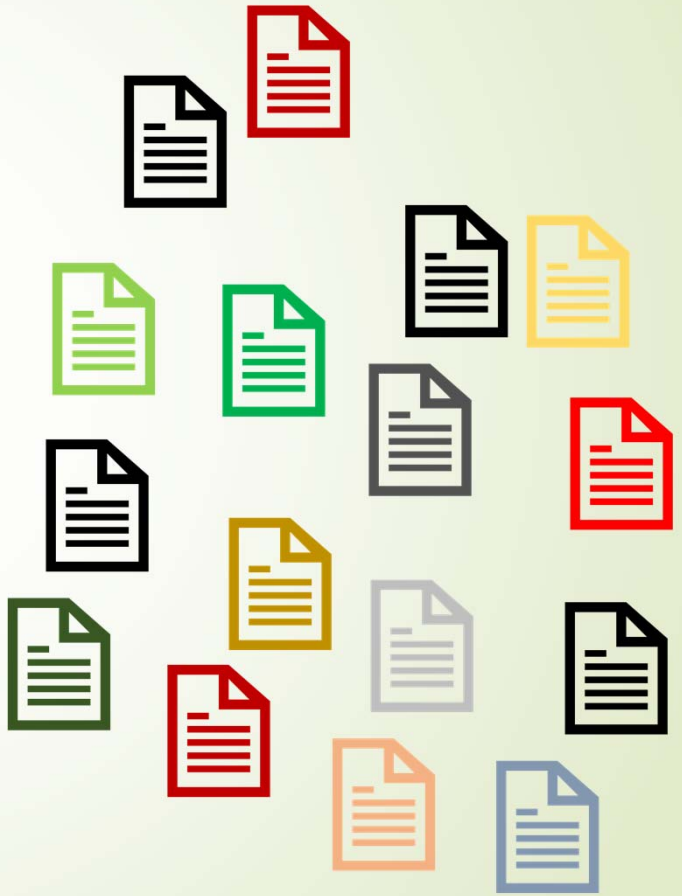
- The laws governing trade secrets differ slightly from country-to-country,
- Common among nearly all these laws is that a trade secret is any information that is...
  - Secret
  - Has value
  - Is subject to “reasonable” protection measures



Examples

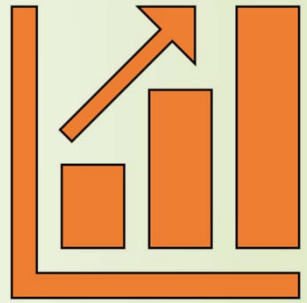
- A trade secret can be a formula, a practice, a process, a design, an instrument, a pattern, a commercial method, a compilation of information, business or financial information, plus much more.

- Trade secrets can even include ‘negative information’.



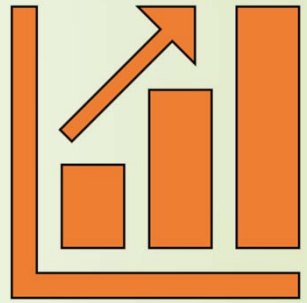
Key trends

- Trade secret protection has become an increasingly important part of the arsenal of protections available for a company's intellectual assets.
- Why?
  - Stronger federal protection under the Defend Trade Secrets Act ("DTSA")
  - The ability to protect a wide range of valuable information, including information that would not be eligible for protection under existing patent, trademark, or copyright law,
  - The time, cost, and uncertainty inherent in the patent application process and a reluctance to disclose one's "secret sauce,"
  - The ubiquity and transportability of data and increased importance of data and data-based analysis and technologies.



Key trends

- Enhanced trade secret laws in key jurisdictions.
- Increased trade secret litigation.
- Trade secrets being shared more thanks to open or collaborative forms of innovation.
- Trade secrets being integrated into major trade agreements.
- The tax authorities are taking greater interest
- IP reform in key jurisdictions is challenging other forms of IP (e.g. patents)
- The very nature of employment is changing, with people switching jobs more often
- Cyber criminals are trying to steal trade secrets



Key Concept: Reasonable protection

- Many companies look at protection as static
- A good approach to ‘reasonable protection’ is to ‘wrap’ the information in layers of protection …
  - Administrative measures
  - Legal measures
  - Technical & physical measures

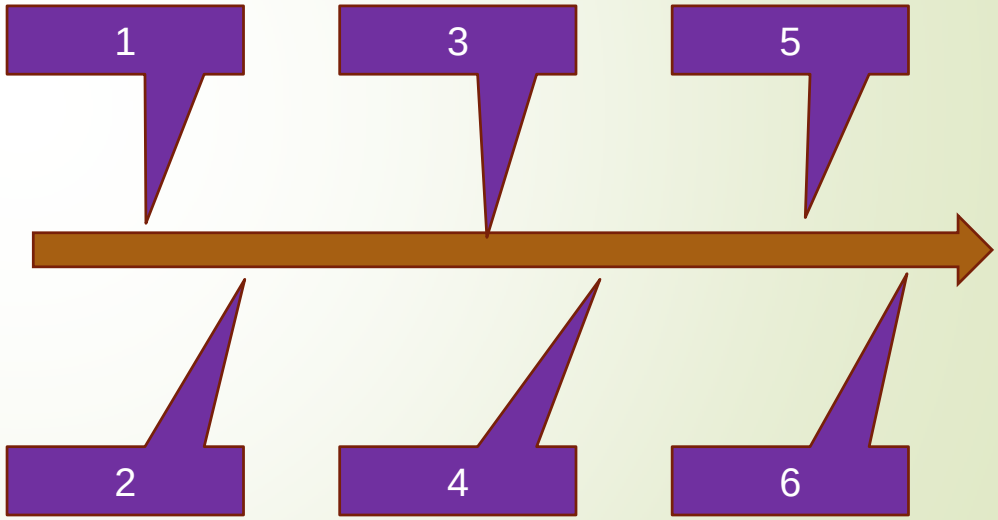
Proper Trade Secret Management

- Proper trade secret protection of intellectual assets – one that will be able to most effectively guard against misappropriation and allow a company to pursue an enforceable remedy in instances of misappropriation - requires a approach that is:
  - proactive,
  - holistic,
  - multi-pronged management approach.

- This presentation examines considerations for an effective trade secret asset management through the lens of trade secret misappropriation We will examine how to approach the questions of:
  - what to protect as a trade secret, and
  - how and whether a company would safeguard and enforce its IP if there were a misappropriation.

The six stages for consideration

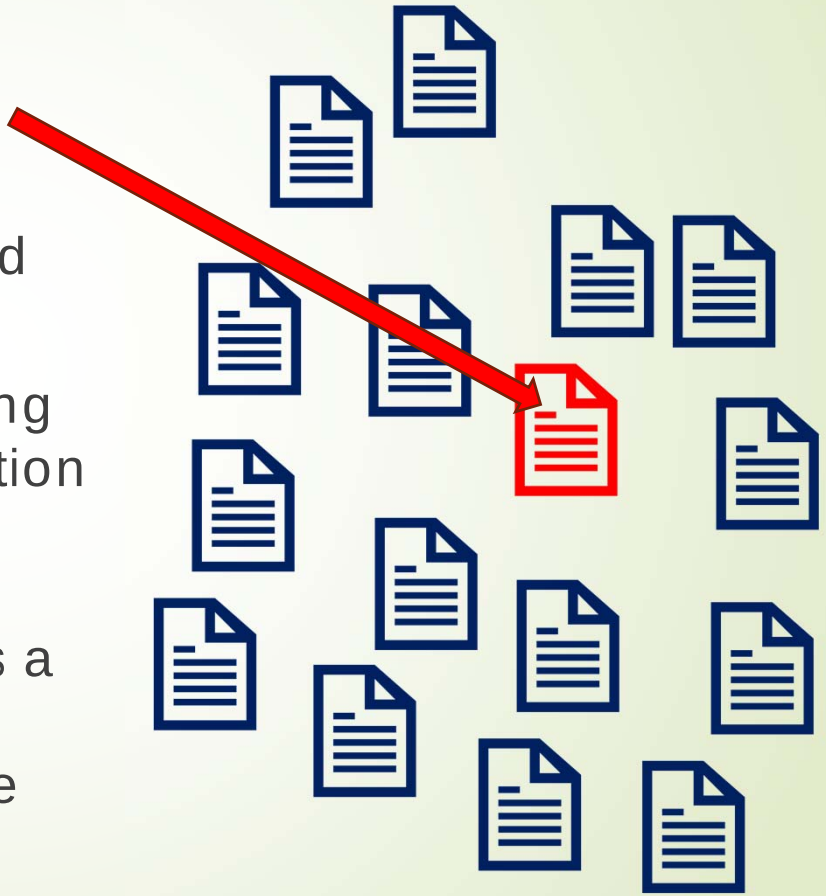
- Looking from the point of view of enforcement, there are six sequential stages of consideration:
  - Recognition
  - Detectability
  - Provability
  - Specificity
  - Correlation
  - Mitigation



NB: Any similarity to “The Six Stages of Grief” is purely coincidental. In fact, following these six stages is designed to avoid grief on the part of the trade secret holder when the time arises to pursue a claim of trade secret misappropriation.

Stage 1: Recognition

- Here the trade secret owner recognizes that they have a protectable trade secret and considers how to protect it.
- The first requirement in proving a trade secret misappropriation case is for the trade secret holder to establish that the information is protectable as a trade secret and that "reasonable measures" were taken to keep it secret.

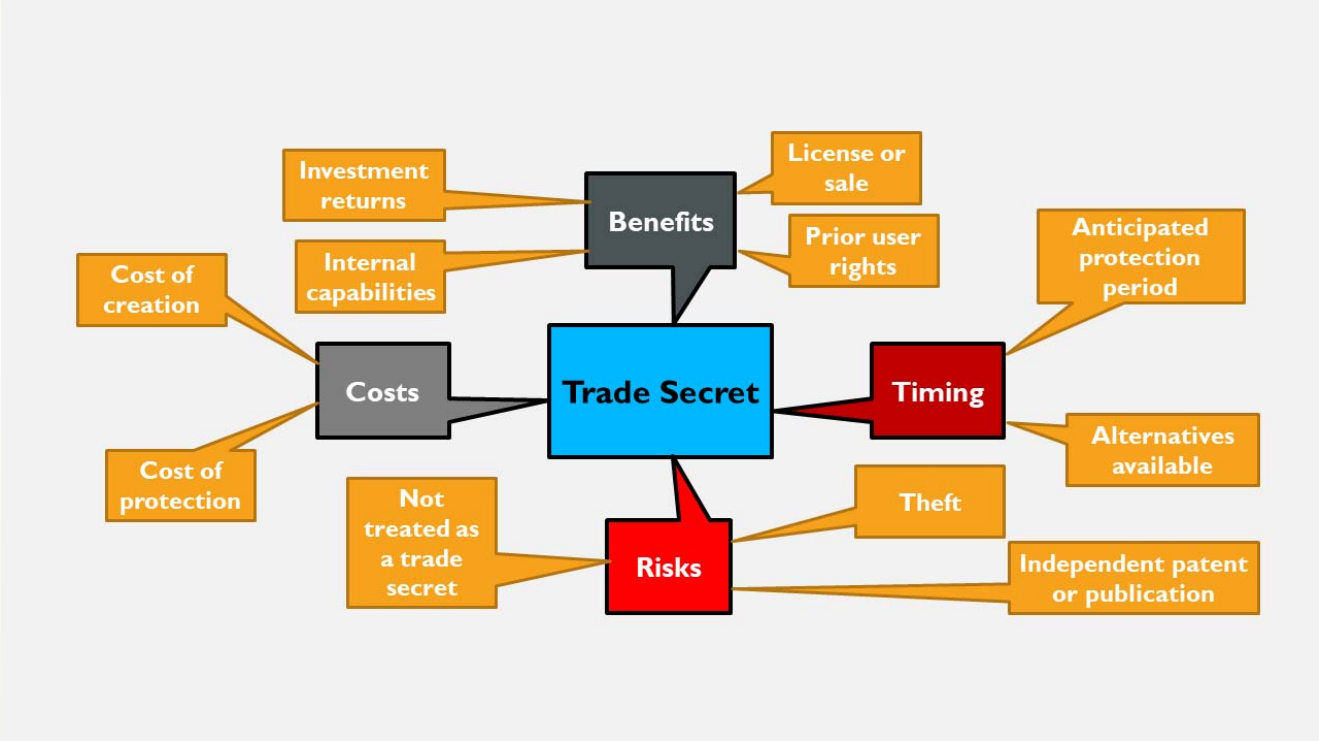


Delving deeper into recognition

- What is "reasonable" depends on the circumstances. There is no "bright line" test under the DTSA for what constitutes reasonable measures.
- Measures to maintain secrecy may include both legal and technological protections.
  - On the legal side, what is the company policy regarding who has access to the information? Is it marked Confidential or Highly Confidential and governed by non-disclosure obligations?
  - On the technology side, how is limited access enforced and maintained? Factors that are considered in determining whether the measures a company put in place were sufficiently reasonable include the cost and effort in acquiring the information, the value of the information, the level of competition in the marketplace, and how easy it is to reverse-engineer.

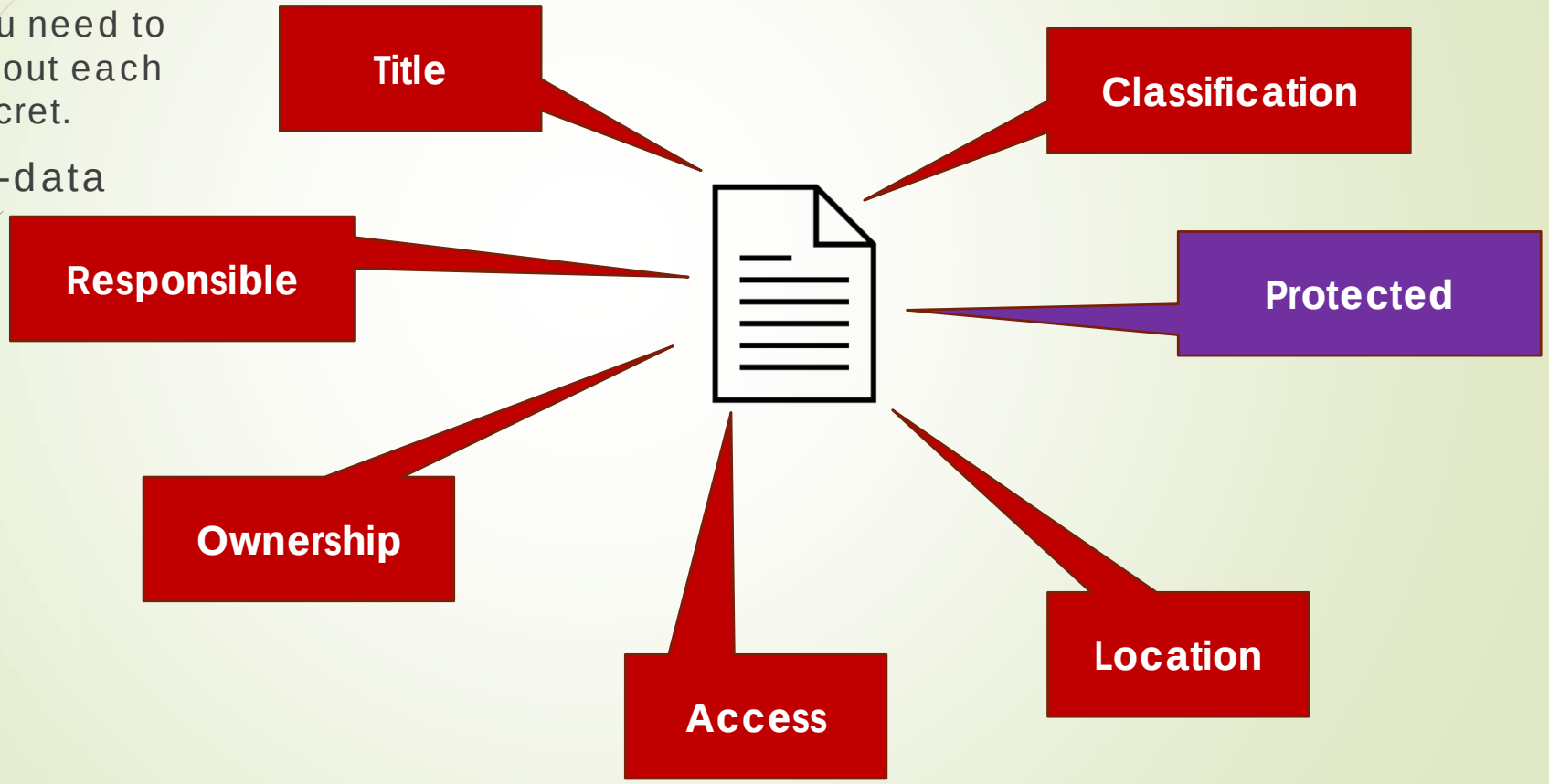
Delving deeper into recognition

- Recognition should also consider ***valuation***.
  - For a secret to be a trade secret under the law it must derive some economic value from being secret.
  - Recognizing the ranges of values of trade secrets can also help to prioritize allocation of resources and make decisions as to how to safeguard the most important assets.



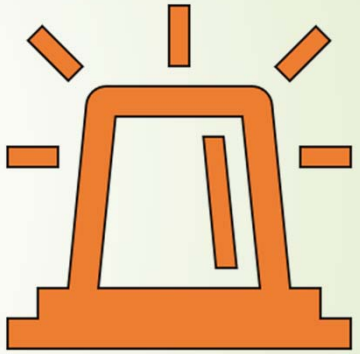
Delving deeper into recognition

- The basics:
  - What you need to know about each trade secret.
- Core meta-data



Stage 2: Detectability

- Once a trade secret owner has put a trade secret protection regime in place, the owner needs to next consider consider what processes or tools it will put in place to monitor and determine whether the trade secret has been compromised or stolen.
- Various technical solutions exist.



Delving deep into detectability

Trade secret theft

Your own employees

Your own Directors & Officers

Your collaboration partners

Suppliers, Customers

Your competitors

Government entities

Hackers & cyber criminals

- Some companies mistakenly assume that the risk is only from outside threats.
- Understanding where the bad actors are coming from and where you are potentially vulnerable informs your choices as to how to protect yourself.

Stage 3: Provability

- Once a trade secret owner has detected a misappropriation, the next concern is being able to prove in a legally sufficient way that there was in fact a misappropriation.
- While legal sufficiency will vary between legal jurisdictions, non-manipulatable proof of a misdeed is always preferred.

Delving deeper into provability

- "Trust me your Honour" is not sufficient, your need evidence.
  - Evidence can include time-stamped and encrypted video logs, or notarized affidavits chronicling security protocols made prior to any particular suspicion of a theft arose.
  - Evidence that the trade secret were handled improperly (e.g., saving the information to a USB drive, laptop, or sending it as an email attachment) can also be of great value.

Stage 4: Specificity

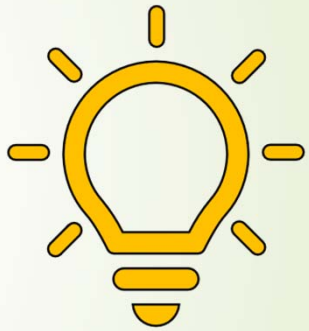
- Once a trade secret owner can prove that there was a misappropriation, they will need to tie that misappropriation to a particular bad actor.
- This is about being able to pinpoint specific entities or people that were involved in the breach.

Delving deeper into specificity

- For example, being able to show that a particular user or IP address was used to access a company's server should be enough for the owner to convince a court to grant legal discovery of the user or IP address or *ex parte* collection of other evidence — and perhaps temporary injunctive relief.

Stage 5: Correlation

- Once a trade secret owner can tie a misappropriation to a bad actor, the next step is to show that is more likely than not that the bad actor possesses the trade secret due to misappropriation and not due to their independent invention.



Delving deeper into correlation

- It is not always the case that there was misappropriation when a competitor releases a markedly similar product to the trade secret owner's product.
- In general, the trade secret owner will ultimately still bear the burden of proof that defendant did not independently invent the trade secret.
- The ability of the trade secret owner to specifically establish when, where, who, and how the trade secret was misappropriated can be important to meet this burden.

<u>Techniques</u>

Watermarking

Paper towns

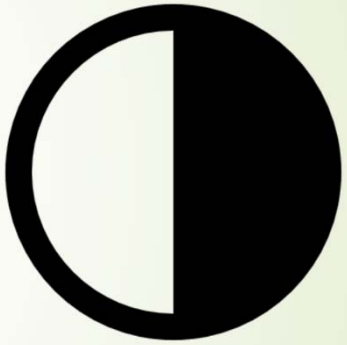
Easter eggs

Stage 6: Mitigation

- Once an owner's trade secrets have been misappropriated, what can be done to minimize the damage from its possession by bad actors?
- This stage addresses how to structure and share trade secrets in such a way that make it hard for a thief to fully exploit them.

Delving deeper into mitigation

- One approach used here is to divide or split the trade secret into parts
  - Only give portions of a trade secret to any one recipient, such that the portion of the secret shared cannot be used to fully exploit the value of the entire secret.
  - Another, in the outsourced manufacturing context, is structuring manufacturing processes so that the manufacturing process is conducted in stages, at different locations, with (possibly) different OEMs.

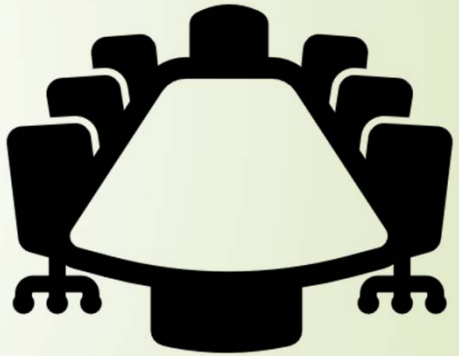


The ‘six stages’ framework

- Reviewing trade secret misappropriation through the lens of these six stages should help to provide a framework that illuminates your potential vulnerabilities and reveals what steps should be taken to shore up your or your client’s trade secret protections.

Trade secret asset management

- Trade secret education
- Trade secret policies
- A process for handling trade secrets
- Protection mechanisms
- Trade secret asset management system
- Trade secret metadata
- Trade secret governance



Thank you