PROGRAM MATERIALS
Program #30246
November 18, 2020

The Six Stages of Trade Secret Misappropriation Protection

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

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.

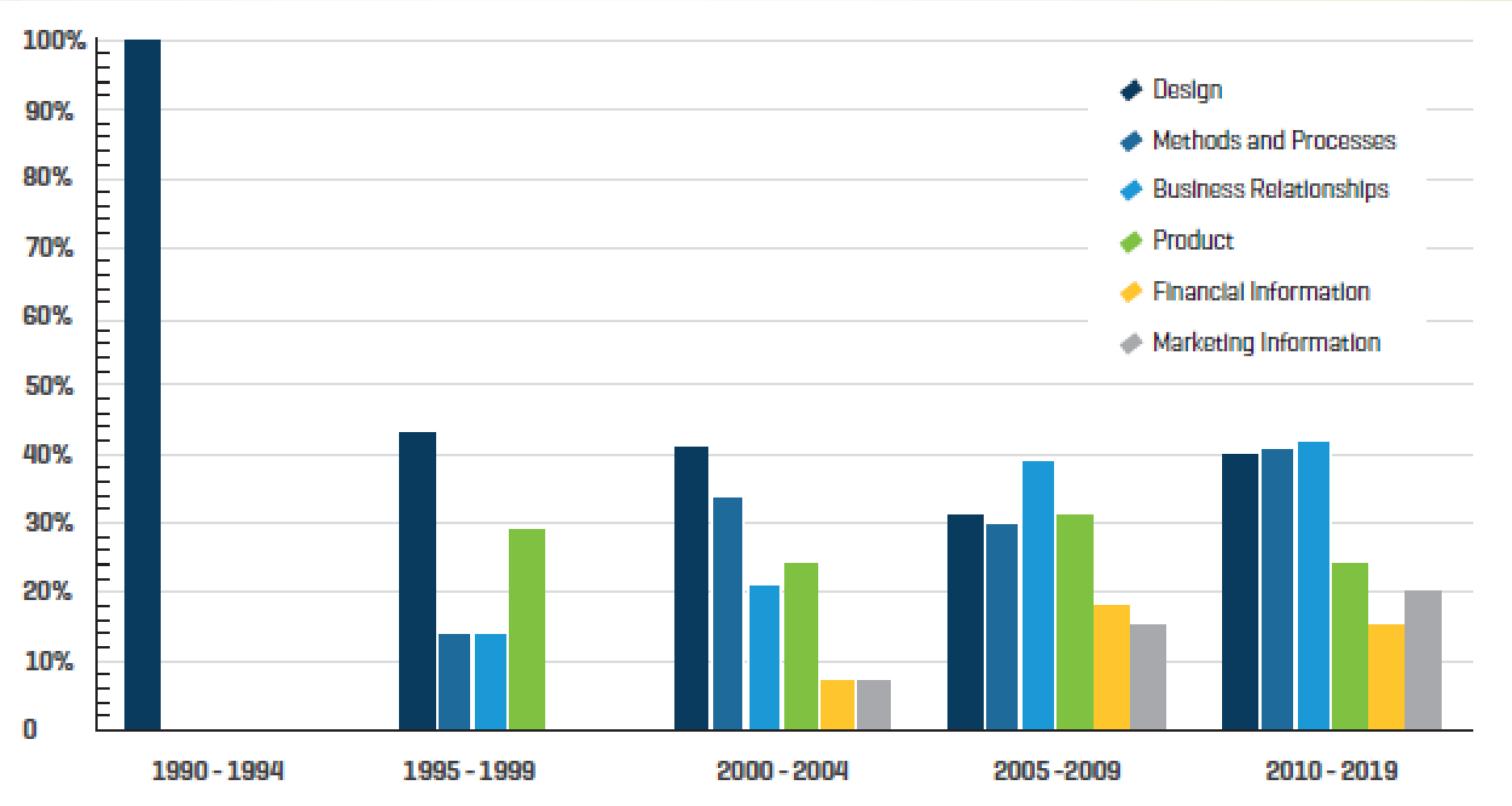
Trade Secret Basics

- 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—

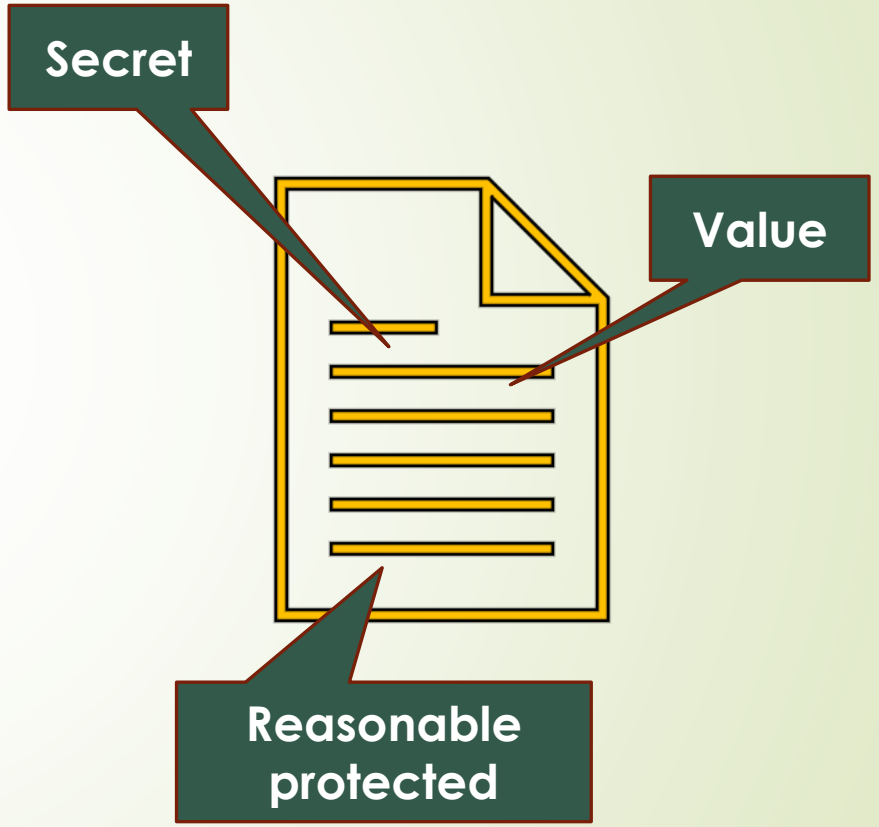
(A) the owner thereof has taken reasonable measures to keep such information secret; and

(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



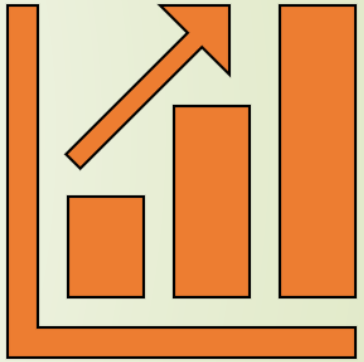
Examples

- 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’.

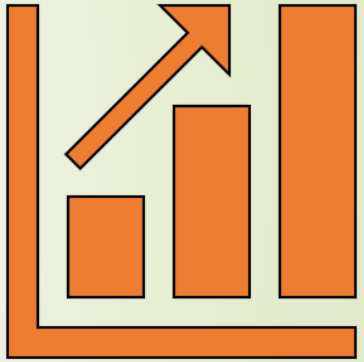
Key trends

- 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

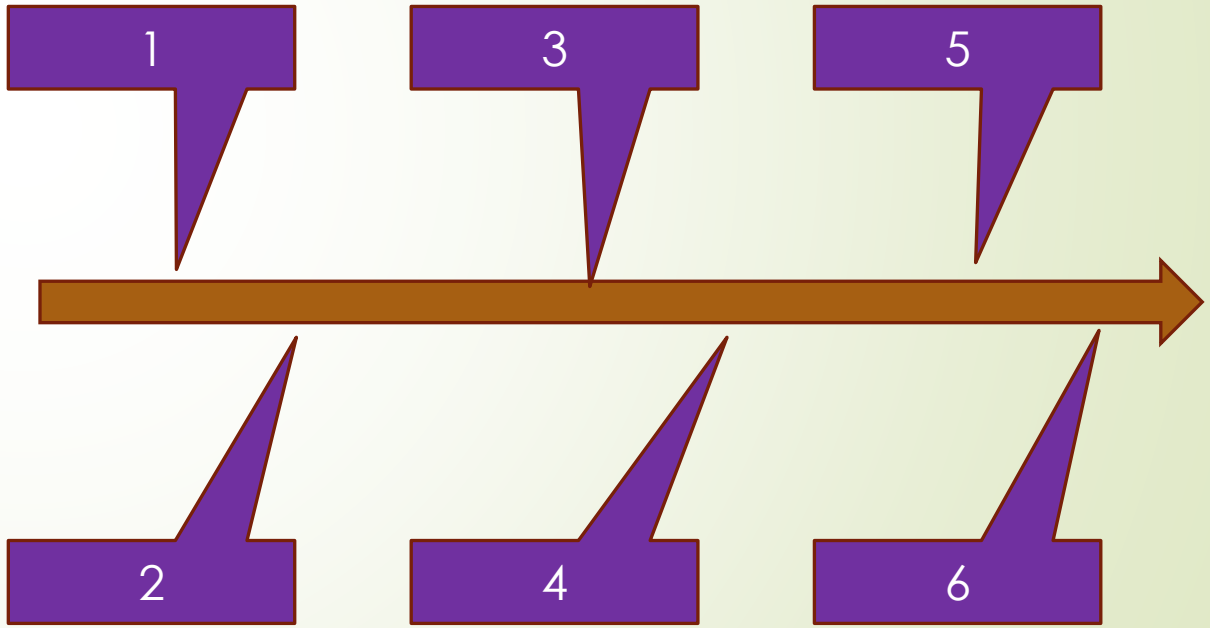
Proper Trade Secret Management

- 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

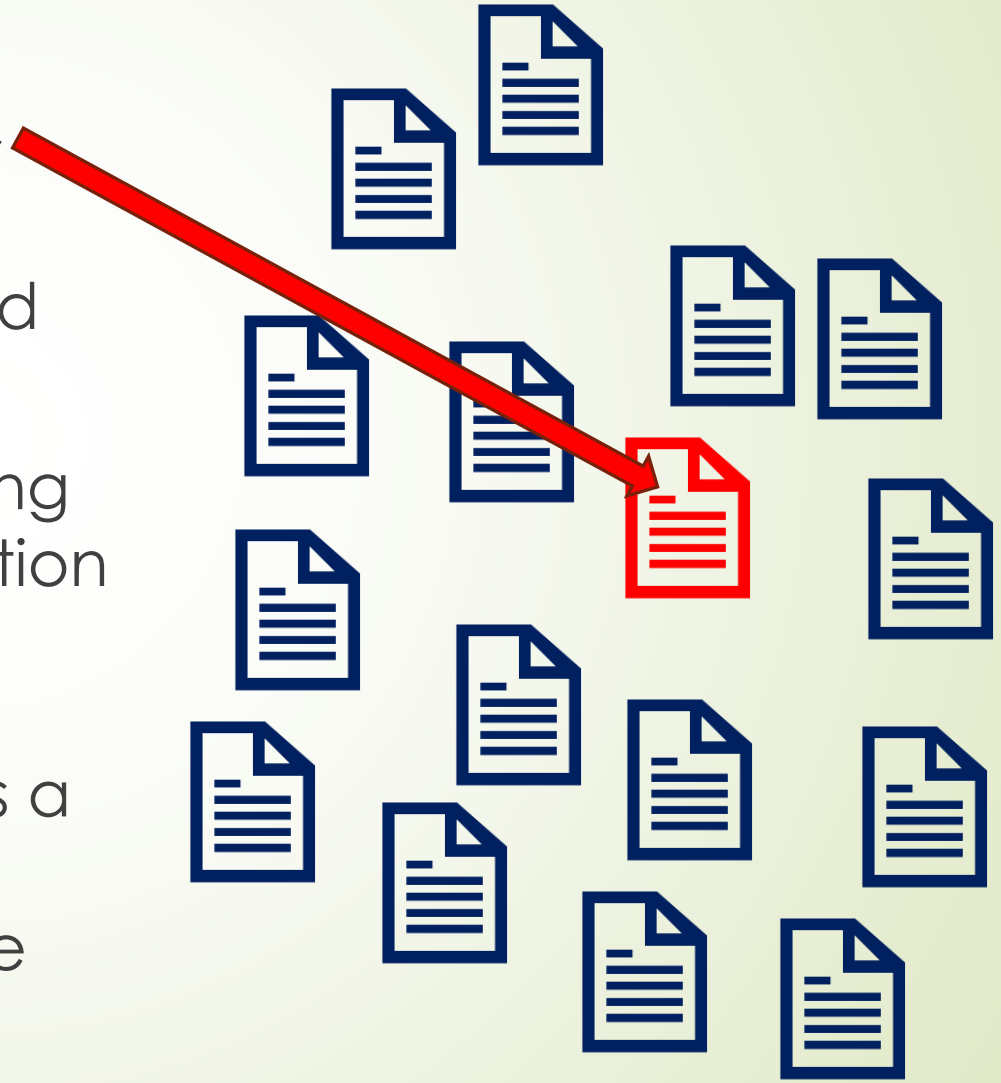
- Looking from the point of view of enforcement, there are six sequential stages of consideration:
  - Recognition
  - Detectability
  - Provability
  - Specificity
  - Correlation
  - Mitigation



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.

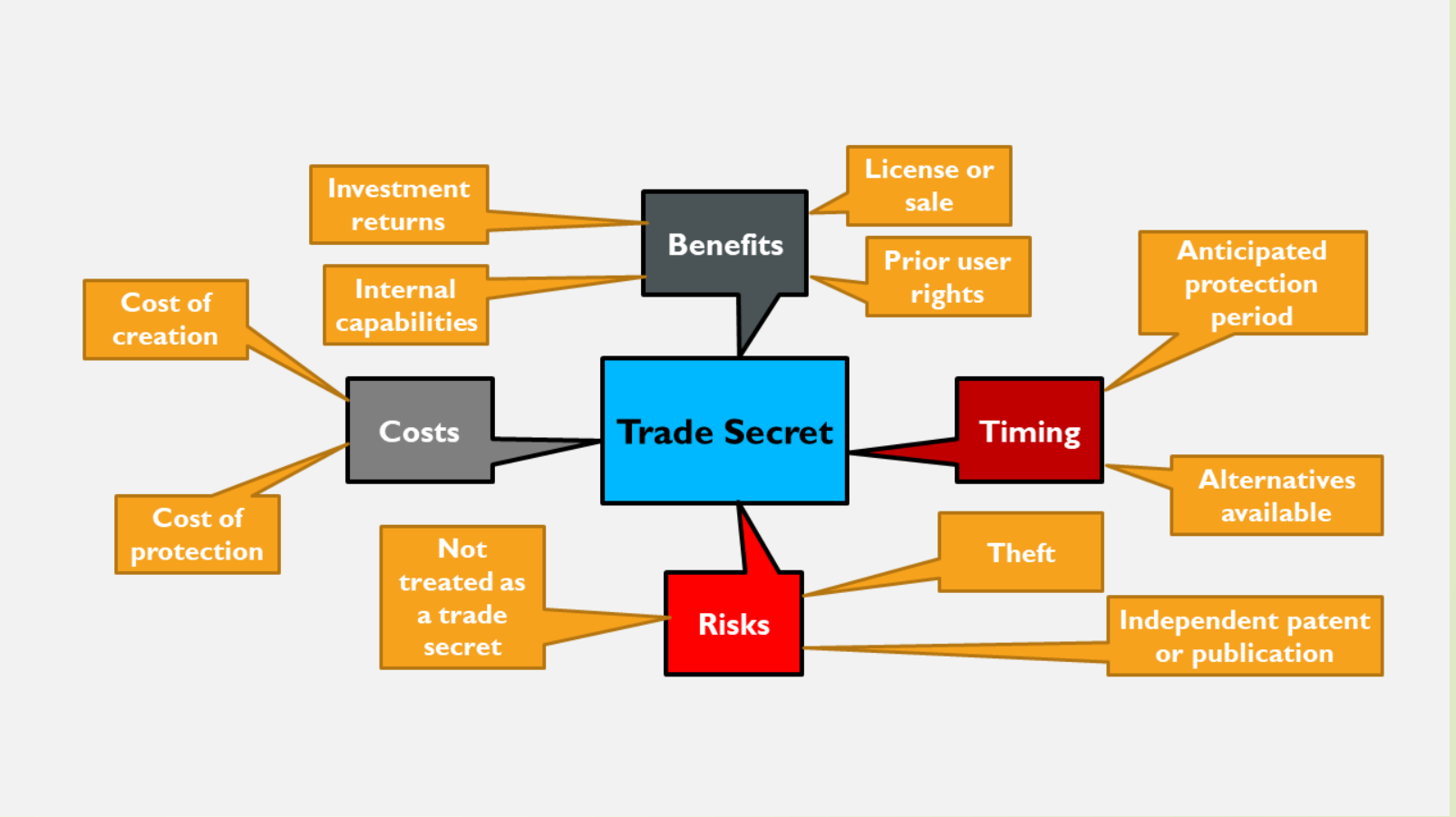


Delving deeper into recognition

- 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.

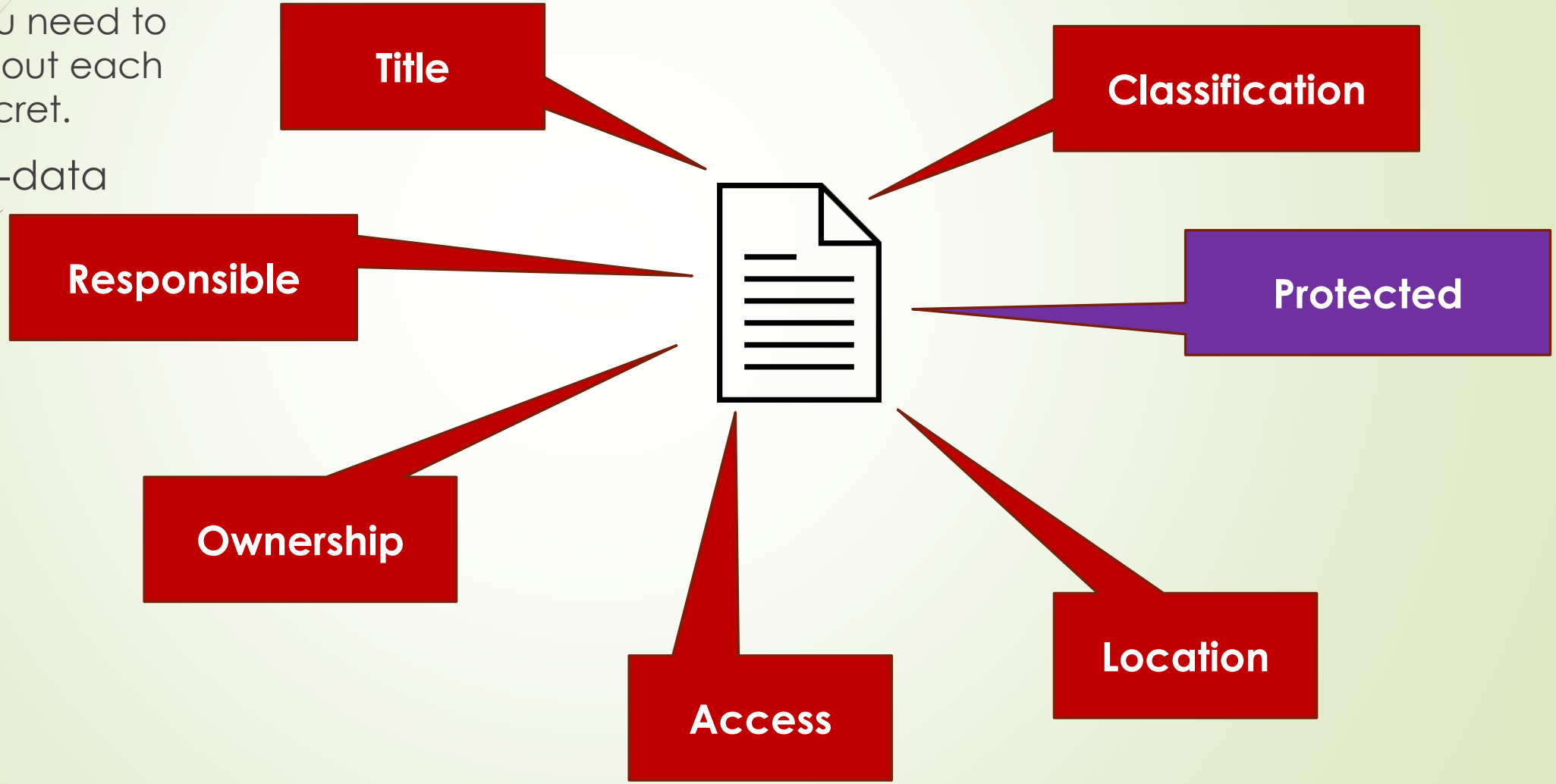
Delving deeper into recognition

- 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.



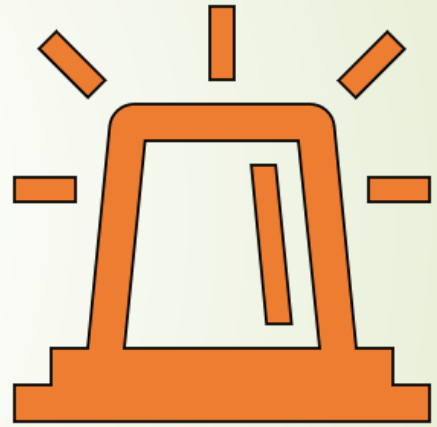
Delving deeper into recognition

- 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

<u>Trade secret theft</u>

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.

Techniques

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

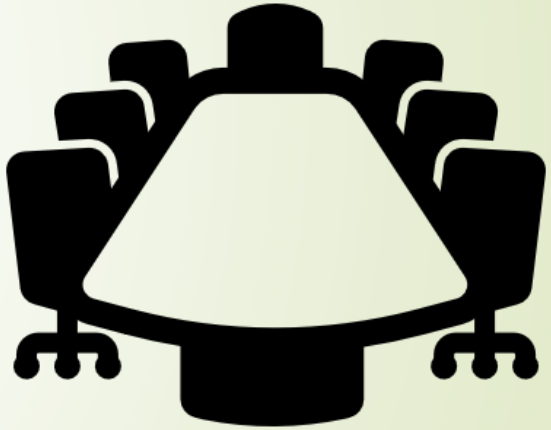
- One approach used here is to divide or split the trade secret into parts
  - Only give portions of a trade secret to any one recipient, such that the portion of the secret shared cannot be used to fully exploit the value of the entire secret.
  - Another, in the outsourced manufacturing context, is 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

OECD BEPS from an IP Management perspective

Jodie Arnold & Donal O'Connell

OECD:

The Organization for Economic Co-Operation and Development (OECD) is at the forefront of efforts to improve international tax co-operation between governments to counter international tax avoidance and evasion.

OECD BEPS:

The OECD / G20 Base Erosion and Profit Shifting (BEPS) package of measures has been agreed upon with over 100 countries and jurisdictions confirming their commitment to consistently implement this comprehensive package. The package provides 15 Actions ranging from new minimum standards to revision of existing standards; common approaches which will facilitate the convergence of national practices and guidance drawing on best practices.

Described by the OECD as "the most significant re-write of international tax rules in a century," the BEPS package provides countries with the powerful tools to standardize compliance requirements and force firms to be transparent about where they generate income

The 15 actions:

These 15 actions were developed to address tax avoidance.

Action 1 - Address the Tax challenges of the Digital Economy

· "These measures are intended to level the playing field between domestic and foreign suppliers and facilitate the efficient collection of VAT due on cross-border business-to-consumers transactions."

Action 2 - Neutralise the Effects of Hybrid Mismatch Arrangements

· "Helps prevent double non-taxation by eliminating the tax benefits of mismatches"

· "Puts an end to costly multiple deductions for a single expense through deductions in one country without corresponding taxation in another"

· "Puts an end to the generation of multiple foreign tax credits for one amount of foreign tax paid"

Action 3 - Strengthen Controlled Foreign Company Rules

· "Ensures that jurisdictions that choose to implement them will have rules that effectively prevent taxpayers from shifting income into foreign subsidiaries"

Action 4 - Limit Base Erosion via Interest Deductions and Other Financial Payments

· "Ensures that an entity's net interest deductions are directly linked to the taxable income generated by its economic activities and fostering increased coordination of national rules in this space."

Action 5 - Counter Harmful Tax Practices More Effectively, Taking into Account Transparency and Substance

· "Ensures that taxpayers benefiting from preferential IP regimes did in fact engage in research and development and incurred actual expenditures on such activities"

Action 6 - Prevent Treaty Abuse

· Treaty here refers to individually negotiated bargains between sovereign states

· "provides a minimum standard on preventing abuse including through treaty shopping and new rules that provide safeguards to prevent treaty abuse"

Action 7 - Prevent the Artificial Avoidance of permanent establishment status

· "These changes address techniques used to inappropriately avoid the tax nexus, e.g. companies doing business in a state to collect and pay taxes in that state"

Action 8 - Assure that Transfer Pricing Outcomes are in Line with Value Creation - the arm's length principle

· "Provides an approach to ensure the appropriate pricing of hard-to-value-intangibles has been agreed upon within the arm's length principle"

· An arm's length transaction is one in which the parties involved are independent and on equal footing

Action 9 - Assure that Transfer Pricing Outcomes are in Line with Value Creation - allocation of risk

· "Provide contractual allocations of risk with appropriate decision-making and control"

Action 10 - Assure that Transfer Pricing Outcomes are in Line with Value Creation - commercial IP movement for tax avoidance

· "Prevent profit allocations resulting from controlled transactions which are not commercially rationale"

· "Prevent the use of transfer pricing methods as a way of diverting profits from the most economically important activities of the MNE group"

Action 11 - Measuring and Monitoring BEPS

· "Provides better tax data and analysis to support the monitoring of BEPS including analytical tools to assist countries in evaluating the fiscal effects of BEPS and impact of BEPS countermeasures for their countries."

Action 12 - Require Taxpayers to Disclose their Aggressive Tax Planning Arrangements

· "Provides a modular framework of guidance for use by countries without mandatory disclosure rules which seeks to design a regime meeting the countries' need to obtain early information on aggressive or abusive tax planning schemes"

Action 13 - Re-examine Transfer Pricing Documentation

· “Requires MNEs to provide tax administrations with high-level information regarding their global business operations and transfer pricing policies in a “master file” that is to be available to all relevant tax administrations.”

· “Require that detailed transactional transfer pricing documentation be provided in a “local file” specific to each country”

· “Requires large MNEs to file a Country-by-Country annual report for each tax jurisdiction, which should contain the amount of revenue, profit before income tax, income tax paid and accrued and other indicators of economic activities”

Action 14 - Make Dispute Resolution Mechanisms More Effective

· “Provides a minimum standard for the resolution of treaty-related disputes.”

Action 15 - Develop a Multilateral Instrument

· “Explores the technical feasibility of a multilateral instrument to implement the BEPS treaty-related measures and amend bilateral tax treaties”

Looking at these actions, it is clear that the OECD BEPS guidelines are not just about tax, they can be seen as an IP management handbook, dictating how companies should behave when managing their intangible assets.

Emphasis on intangible assets:

An essential feature of the new regulations is an emphasis on intangible assets. It is increasingly recognized that intangible assets create a substantial part of the business value. However, until now there has been no single definition of Intangible Assets in use by tax authorities or the OECD, and no proper guidance on how such assets should be reported.

The accurate and complete identification, taxation and valuation of intellectual property and other intangible assets is now recognized as one of the most important areas of the international tax reform and transfer pricing legislation.

Assessing compliance:

Compliance means conforming to a rule, and the OECD guidelines clearly define new rules as far as a MNE’s IP management is concerned. Assessing compliance is an activity to determine, directly or indirectly, that a process meets relevant standards and fulfils relevant requirements.

It’s suggested that MNEs will need to conduct an exercise now or in the near future to determine if they are OECD BEPS compliant or not, and if not, to then take the necessary actions to ensure compliance.

It’s also suggested that such a conformity assessment may be broken down into at least 7 parts. (There may be other parts to be added).

· Qualification

· Definition of intangible assets

· IP data management

- Maturity of the MNE's IP processes and systems
- Transfer pricing
- Reporting
- Exceptions

Qualification:

The OECD guidelines apply to all multinational enterprises. An MNE is defined as an organization that owns or controls production of goods or services in one or more countries other than their home country.

Several of the OECD measures have been crafted in such a way as to minimise the impact on SMEs with negligible BEPS risks.

This part of the conformity assessment simply sanity checks if the company is a MNE as defined by the OECD and as far as OECD BEPS guidelines are concerned.

Certain tax jurisdictions may apply OECD BEPS guidelines to smaller enterprises, and there is evidence that this is certainly happening.

Definition of intangible assets:

In the OECD guidelines, it defines intangible assets as including the following categories

- Patents
- Know-how and trade secrets
- Trademarks, trade names and brands
- Rights under contracts and government licenses
- Licenses
- Goodwill

The OECD guidelines also specifically exclude certain items from being considered as intangible assets as far as OECD BEPS compliance is concerned.

This part of the conformity assessment compares and contrasts the OECD's definition of intangible assets to that definition in active use within the company and identifies any differences which require further examination.

IP data management:

Within Action Plan #8, the OECD describes a number of IP data management related tasks required of the MNE.

- Identification of all intangible assets
- Ownership of all such assets

- Contribution by group members
- Re-imbursement by the legal owner to other group members for their contribution
- Valuation of such assets
- Agreements in place between group members
- Arms-length fees and fee structures agreed

This part of the conformity assessment checks if the MNE has the skills and competencies, knowledge and experience, process and systems in place to enable the MNE to complete these IP data management related tasks, and if not, what actions need to be taken to remedy the situation.

Maturity of IP processes and systems to support OECD BEPS compliance:

Any MNE will need to be at a certain level of IP maturity and sophistication in order to be OECD BEPS compliant.

- Awareness & education
- Processes
- Systems
- Data
- Data integrity
- Governance

This part of the conformity assessment reviews the maturity and sophistication of the IP processes and systems in use for each category of intangible asset within the MNE and identifies any gaps as far as the MNE being OECD BEPS compliant from an IP perspective.

Transfer pricing:

Transfer pricing is the setting of the price for goods and services sold between controlled (or related) legal entities within an enterprise. As far as OECD BEPS is concerned, it is the setting of the price for intangible assets being licensed by one member of the group to other member(s) of the group.

The guidance on transfer pricing documentation requires MNEs to provide tax administrations high-level global information regarding their global business operations and transfer pricing policies in a “master file” that would be available to all relevant country tax administrations.

It also requires that more transactional transfer pricing documentation be provided in a "local file" in each country, identifying relevant related party transactions, the amounts involved in those transactions, and the company’s analysis of the transfer pricing determinations they have made with regard to those transactions.

MNEs will be required from an IP perspective to:

- Identify intangible assets linked to the licensing of intangible assets between group members.

· Determine the valuation given to such intangible assets and the valuation methodology used

· Gather details on all such licenses between group members.

· Demonstrate that they have used arms-length fees and fee structures when deciding on the pricing.

· Check that the IP terms and conditions in such agreements are reasonable, and not adversely impacting OECD BEPS compliance.

If there are significant numbers of such arrangements in place within the group, the conformity assessment will also review and check that the MNE has the following in place:

· Processes for creating and managing such agreements

· System(s) to underpin such processes

· Metadata associated with such agreements

· A governance structure in place

Reporting:

The OECD specifically asks for the following information to be reported within a Master file:

· A general description of the group's overall strategy for the development, ownership and exploitation of intangible assets

· A list of intangibles, or groups of intangibles, that are important for transfer pricing purposes

· Details of those entities that legally own the intangibles

· A list of important agreements among identified associated enterprises within the group related to intangible assets.

· A general description of the group's transfer pricing policies related to intangible assets.

· A general description of any important transfers of interests in intangible assets among associated enterprises within the group during the fiscal year concerned, including the entities, countries, and compensation involved.

This part of the conformity assessment checks if the MNE is capable of producing such reports in a proper and professional manner and identifies any gaps which need addressing.

Exceptions:

There are a number of exceptions which need to be considered when conducting a conformity assessment.

· Exceptions outlined within the OECD BEPS guidelines

· Exceptions specified by national governments when they implement the OECD BEPS guidelines

· Exceptions due to corporate events of the MNE being assessed

Far from theoretical:

You may believe that this is all very theoretical and that your company does not have to concern itself with OECD BEPS compliance.

However, this issue is already impacting companies. Just in the past few weeks alone, we are aware of the following developments ...

Case #1:

An MNE in the automotive sector HQ'd in Europe and with production facilities off shore was recently audited by the tax authorities from a major European country. The tax folks were especially focused on the company's OECD BEPS compliance with respect to their patents and trade secrets, and how these IP assets flow between HQ and their production facilities in other tax jurisdictions.

Case #2:

An Israeli based high tech SME with their parent company in Europe is currently being challenged by the Israeli tax authorities with respect to how the IP generated by the SME is being handled, the relationship between the 'parent' company and the 'child' company in terms of IP in intergroup licenses and transfer pricing, and how the SME is being compensated for this contribution to the company as a whole. In this case, the IP is mostly a mix of patents and trade secrets.

Case #3:

A Chinese MNE is in the process of establishing an IP Holding company (mostly involving trade secret assets) and wants to ensure that it is OECD BEPS compliant. However, it also wants to ensure that it complies with all export controls related to its technology.

Case #4:

An MNE in the chemical and consumer goods sectors is wanting to update its IP data management system to ensure that it incorporates OECD BEPS functionality

Final thoughts

We trust that the above information is of interest and of value, especially since this is “the most significant re-write of international tax rules in a century”. These OECD BEPS guidelines are not just about tax, they can be seen as an IP management handbook, dictating how companies should behave when managing their intangible assets.

The Six Stages of Trade Secret Misappropriation Protection

Article by David L. Cohen, Michael Kasdan & Donal O'Connell

Trade secret protection has become an increasingly important part of the arsenal of protections available for a company's intellectual assets. The reasons for this are many and include: (i) stronger federal protection under the Defend Trade Secrets Act ("DTSA"), (ii) 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, (iii) the time, cost, and uncertainty inherent in the patent application process and a reluctance to disclose one's "secret sauce," and (iv) the ubiquity and transportability of data and increased importance of data and data-based analysis and technologies.

When considering how to protect their trade secrets, many companies typically begin and end their analysis with putting a valid non-disclosure agreement in place when communicating with third parties about their proprietary technologies. This approach, as we have **discussed** elsewhere, is necessary but not sufficient. Rather, 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 proactive, holistic, and multi-pronged management approach.

This article examines considerations for an effective trade secret asset management through the prism of trade secret misappropriation, examining how to approach the question 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.

There are six sequential stages of consideration: Recognition, Detectability, Provability, Specificity, Correlation, and Mitigation. (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.)

THE FIRST STAGE IS RECOGNITION.

In this first stage, 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 (i.e., that it is not generally known or ascertainable and has economic value) is that **"reasonable measures"** were taken to keep it secret. There is no "bright line" test under the DTSA for what constitutes reasonable measures; **what is "reasonable" depends on the circumstances**. Measures to maintain secrecy may include both legal and technological protections. For example, 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.

An important part of recognition is to begin to consider valuation. For a secret to be a trade secret under the law it must derive some economic **value from being secret**. Thus, the trade secret owner must be able to show that the secret had or has value, and that its value was based – at least in part – on it being secret. While the absolute dollar threshold required to be considered a trade secret is relatively low, getting a sense of what the secret is worth will be very useful should the owner need to seek **damages**. **Sophisticated trade secret owners** will keep track not only of the value of their secrets but the costs associated with keeping them secret – both for internal controls and to assist in later valuation and potentially pursuit of damages in the event of a misappropriation. Recognizing the ranges of values of trade secrets can

CONTINUED

also help to prioritize allocation of resources and make decisions as to how to safeguard the most important assets.

THE SECOND STAGE IS DETECTABILITY.

Once a trade secret owner has put a trade secret protection regime in place, the owner needs to next consider what processes or tools it will put in place to monitor and determine whether the trade secret has been compromised or stolen. Examples of available tools for *detection* range from video cameras to software to detect when confidential files are downloaded to employee laptops or devices without pre-authorization. Some processes include daily physical inspection of the premises where trade secrets are located and monitoring competitor products for suspiciously similarities. One of the most troubling aspects of trade secret asset management is the recognition that most misappropriation comes from your trusted colleagues. While outside threats such as hackers are a serious issue, according to **one survey** of the reported cases, a whopping 82% of cases involve current (55%) or former (27%) employees, more often than not (59%) acting alone. While perhaps a sad commentary on employee loyalty, this fact of life should be viewed as an opportunity to employ common sense measures that both create disincentives to misappropriation such as surveillance (**which can deter and thus reduce theft**) as well as incentives for good behavior (**increased pay and employee satisfaction can reduce theft**).

THE THIRD STAGE IS 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. This can include time-stamped and encrypted video logs, or notarized affidavits chronicling security protocols made prior to any particular suspicion of a theft arose. Indeed, simple technical protections also would do wonders to deter trade secrets – as the same **survey discussed above** showed 45% of all trade secret theft was of files or documents which employees accessed or handled improperly (e.g., saving the information to a USB drive, laptop, or sending it as an email attachment). Accordingly, keeping careful records of key electronic documents (who accessed, where saved, when, etc.) can be critical in building a trade secret case.

THE FOURTH STAGE IS 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. While it is always good to know that there was a security breach, being able to pinpoint *specific* entities or people that were involved in the breach will allow the trade secret owner to take maximal advantage of the various judicial remedies available. 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.

THE FIFTH STAGE IS 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. 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. The ability of the trade secret owner to specifically establish when, where, who, and how the trade secret was misappropriated can be fatal to a defendant's defense of misappropriation claim by arguing independent invention – especially if they could reasonably have done so (e.g., they had similar R&D capacities as the trade secret owner). There is least one **US circuit court opinion** that held that where defendant can reasonably claim independent invention, the trade secret owner will ultimately still bear the burden of proof that defendant did not independently invent the trade secret.

Indeed, many times disgruntled employees will steal trade secrets from their employer and try to leverage possession of those secrets into jobs or money from their former employer's competitors. **One approach** that rights owners can use to protect themselves is to watermark –

CONTINUED

literally or figuratively – their trade secrets, or intentionally include "**Easter Eggs**" such that when an unauthorized third party uses them there will be evidence that their use is unauthorized. For example, there are many, many examples of competitors who used stolen source code and were unsophisticated enough to remove the original owners of the code comments.

THE SIXTH AND FINAL STAGE IS 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 does not refer to taking immediate action and not sleeping on one's rights. While that is also important, 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. For example, only providing trade secrets on a "need to know basis" or to limited recipients; or only giving 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.

Depending on the circumstances, some of these stages are completed sequentially. Other times they are accomplished in parallel – typically in breaches of IT systems, where the same tools may allow the trade secret owner to determine who accessed the system to access which trade secrets, and correlate those trade secrets to a competitor using them to the owner's disadvantage.

We hope that reviewing trade secret misappropriation through the lens of these six stages helps 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.

We believe that forewarned is forearmed and **that auditing your trade secrets asset management** with each of these stages in mind can both shore up existing trade secrets, while also providing an appreciation for intellectual assets you may not have even known you had.

About David Cohen, Michael Kasdan & Donal O'Connell:

David Cohen, Donal O'Connell and Michael Kasdan have been involved with this form of IP for several years.

David Cohen and Donal O'Connell have had over 50 papers published on various aspects of trade secrets and trade secret asset management. They have conducted intense trade secret workshops for a variety of companies and organizations. They have also developed a leading-edge trade secret asset management solution to help clients (operating companies, legal & IP firms, finance & tax firms, and IP insurance providers) manage such assets in a proper and professional manner.

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 management and trade secret misappropriation.

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

Donal O'Connell is ex VP of R&D and ex Director of IP at Nokia; Adjunct Professor of IP at Imperial College Business School and an IAM300 Top Global IP Strategist member for several years.

Michael Kasdan is an IP Partner at Wiggin and Dana LLP and an Adjunct Professor at NYU School of Law. He has been listed as one of the world's-leading IP Strategists in the 2017 – 2019 editions of *IAM Strategy 300 – The World's Leading IP Strategists*. He is the author of the chapter on Patent Licensing and Monetization in the *Oxford Handbook of Intellectual Property Law* (Oxford Press, 2017). He is also the author of the chapter entitled "Dealing in Intellectual Property: What You Need To Know To Get the Deal Done" in *A Practical Guide to Successful Intellectual Property Valuation and Transactions* (Wolters Kluwer Press, forthcoming 2020).