



How to manage trade secrets – *Video Transcript*

Trade Secret Asset Management

[Click here for video](#)

Donal O'Connell:

In this video, we'll look at the practical steps that organizations should take in order to successfully manage their trade secrets. We'll cover the topic of education, policies and governance, and how to use auditing and data to ensure that trade secrets remain just that... secret.

So first, imagine owning a property empire...

One would expect the owner of any such property empire to have some facts and figures about the various properties in the portfolio at hand. This might include:

- The types of property in the portfolio (flats, detached houses; semi-detached houses, end of terrace houses, cottages, bungalows, hotels, public houses, restaurants, cafes, sports facilities, retail stores, shopping malls, shops, office buildings, serviced offices, industrial property, office/warehouses, garages, distribution centers, etc.).
- The location of each of the properties in the portfolio.
- The legal status with each of these properties together with any associated property title deeds.
- Details on who is renting or leasing each of the properties.
- Finance and tax details on each of these properties.
- Details on how access to each property is controlled, what security arrangements are in place, etc.
- Insurance details for each property

- Maintenance details on each of the properties.
- And so on...

Now rather than physical assets like property, imagine owning a portfolio of valuable trade secrets.

One would surely expect the owner of any such trade secret empire to have some facts and figures about the various trade secret assets in the portfolio at hand.

If it helps, just walk through the bullet points above replacing the word 'property' with the words 'trade secrets'.

But, why is this important? Although trade secrets have been the neglected step-child of IP, this is slowly but surely changing - for a variety of reasons:

- Law changes (DTSA in the USA; the EU Directive on Trade Secret in Europe; and Anti Unfair Competition Law in China)
- There is a trend towards increased trade secret litigation particularly involving US companies but not exclusively so
- There is growing interest in trade secrets by the tax authorities (OECD BEPS, Patent Box Tax Regimes)
- The ever increasing threat of cyber criminals trying to steal trade secrets
- Companies embracing Open Innovation and sharing trade secrets
- The changing nature of employment
- And... Pending trade wars with some links to trade secret theft

However, many companies are poor when it comes to trade secret asset management. Here's some of the common reasons why:

- Trade secrets are poorly managed
- There is a lack of ownership
- Documentation is poor.
- Protection mechanisms are poor or non-existent.
- There is a lack of any classification of such assets.
- Details on whether trade secrets have been shared is often missing
- Trade secrets not properly addressed in agreements & contracts
- There is no audit trail.

Such companies possessing trade secrets fail to appreciate that they need to act as if they own a property empire.

Learning to cycle:

There's an easy way to learn how to cycle. It basically involves getting on the bike and learning by trial and error.

Yes one can read about cycling, watch educational videos, talk to others who can cycle, study all of the components of a bicycle, take a Physics degree, etc. but one should note that one cannot learn to cycle without actually getting on a bike and learning by doing about balance and coordination.

I suggest that the same applies to trade secret asset management. Yes, organisations can read about trade secret laws, digest published case studies, talk to other companies who are doing it well, and so on and so forth... But at some point I suggest that the organisation will just have to get on the bike and learn by trial and error about balance and coordination with respect to these valuable but fragile assets.

I also suggest that trade secret asset management involves at least the following components:

- Education of employees about trade secrets
- Trade secret policy

- Trade secret process
- Trade secret metadata
- And... Trade secret governance

Education of employees:

The importance of education of employees about trade secrets cannot be stated enough. It is a self-enlightening process. It is crucial to the overall development of the individual participant and the company or organization at large. Trade secret education provides the participant with knowledge about the world of trade secrets, and enables informed decisions to be made.

Trade secret education makes the participant capable of interpreting things rightly and applying the gathered information in real life scenarios. Trade secret education is not limited to the course material or case studies. Real trade secret education is obtained from then taking these learnings into use in real life situations.

Yes the organisation's first attempt at educating all of their employees about trade secret may not be perfect. But that interaction with employees is really valuable.

What questions were asked? What concerns were raised? How should the course material and delivery be improved? Who needs more advanced trade secret training? Is the training on trade secrets in alignment with how other forms of IP are handled?

Trade secret policy:

A corporate trade secret policy is a formal declaration of the guiding principles and procedures by which the organisation will operate, typically established by its board of directors, a senior management policy committee or by the Legal or IP function within the organisation

Yes, the first iteration of the organisation's trade secret policy may need enhancing. It may not properly address all aspects. It may for example have missed required changes to other corporate policies. But creating and deploying such a policy forces an organisation to seriously consider what trade secret asset management means to the organisation.

Trade secret process:

A trade secret process can be seen as an agreement to do certain things in a certain way and the larger the organisation, the greater the need for agreements on ways of working. The trade secret process is like the memory of the organisation, and without such a process, a lot of effort can be wasted and the same mistakes can be repeated.

Yes, the first version of the organisation's trade secret process for the handling of such assets might have some weaknesses. The process may not address all events in the life of a trade secret. Perhaps the first version of the trade secret process does not address the valuation of such assets or the sharing of such assets with 3rd parties. However creating such a process and putting into practice provides an opportunity for great learning.

Trade secret metadata:

Metadata is a set of data that describes and gives information about other data. Metadata is simply data that describes other data. Meta is a prefix that in most information technology usages means 'an underlying definition or description'.

Metadata summarizes basic information about data, which can make finding and working with particular instances of data easier. For example, the name of the author, the date created and the last date modified as well as file type and file size are examples of very basic document metadata.

Some mistakenly believe that because trade secrets are not registered, then the concept of trade secret metadata may not apply. Others mistakenly believe that because trade secrets are meant to be kept secret, then no metadata should exist.

This is... RUBBISH!

Trade secret metadata summarizes basic information about the trade secret, which can make finding and working with this unique form of IP much easier.

Within an organisation, there are many who could benefit from having access to some trade secret metadata, such as C Suite Executives, given that trade secrets are some of the most valuable assets within the company; IT and Security given the issues with cyber security; HR given the many employee issues associated with trade secrets; Finance & Accounts given the financial and tax associated linked to such assets; Sourcing & Procurement as many trade secrets are indeed shared; etc.

Yes, the organisation's first attempts at logging and tracking trade secret metadata may be poor. However, the organisation will quickly learn that having good quality trade secret metadata is crucial. Such metadata serves to provide context and/or additional information about these assets.

"You can have data without information, but you cannot have information without data." – Daniel Keys Moran

Trade secret governance:

Governance is the act of governing. It relates to decisions that define expectations, grant power, or verify performance. In the case of a business, governance relates to consistent management, cohesive policies, proper guidance, well defined processes, KPIs and metrics, and decision-rights for a given area of responsibility.

Trade secret governance is simply about defining the 'rules' for those involved in trade secret asset management within the organisation. It is the process of decision-making and the process by which decisions are implemented (or not implemented). Ideally the process should distinguish between strategic and tactical decisions.

Since trade secret governance is the process of decision-making and the process by which decisions are implemented, an analysis of the governance of trade secrets should focus on the formal and informal actors involved in decision-making and implementing the decisions made and the formal and informal structures that have been set in place to arrive at and implement the decision.

Yes the initial attempts by the organisation at trade secret governance might be amateurish. But this organisation will learn by trial and error what it takes to become really professional with respect to trade secret asset management governance.

Get on your bike!

In the UK, the phrase 'on your bike!' is slang, and a rude way of telling someone to go away: "Can you lend me some money?" "On your bike, mate!". This is not my meaning here.

Rather, I am suggesting that organisations need to get on their bikes and learn about trade secret asset management, learning by trial and error about balance and coordination with respect to these valuable but fragile assets.

Trade secrets have been the neglected step-child of IP. Historically, little thought, other than perhaps a non-disclosure agreement, was given to valuing and protecting trade secrets. The current legal and political landscape makes the old approach untenable.

The law is changing - The Defend Trade Secrets Act passed in the USA in May 2016; The EU Directive on Trade Secrets is enacted by member state on 9 June 2018; China enhanced its trade secret laws in early 2018 with revisions to its Anti Unfair Competition Law.

Changes in the eligibility requirements and enforcement mechanisms of patent laws around the world, but especially those in the US – and especially as they relate to software and business methods, make trade secrets an attractive mechanism to protect a company's competitive advantages

Then, there is cyber-crime – whether from competitors or State actors – are working overtime to trying to steal trade secrets from organisations

Also... More and more companies are embracing open and outsourced innovation models which necessarily requires sharing and collaborating on trade secrets with others.

What about employment? Changes in employment models are leading to a highly mobile and transitory workforce where companies have increased risk their employees being poached by actual or potential competitors often with the goal of leverage the employee's trade secret-rich know-how.

There is also growing interest in trade secrets by the tax authorities - OECD BEPS Guidelines include trade secrets as an intangible asset requiring proper management; Patent Box Tax Regimes in a number of jurisdictions now allow trade secrets as qualifying IP; The US Government is encouraging US companies to repatriate their IP back to the US.

Last but not least, we are seeing increased trade secret litigation especially for US companies but not exclusively so.

In short, organisations need to get on their bikes.

Auditing:

One crucial aspect of trade secret asset management is auditing. An audit is the examination of a specific aspect of an organization, ideally by someone independent of that organization.

Conducting an audit is akin to taking a long hard look at ourselves in the mirror, standing in front of our honest selves and taking some time for introspection, seeing if you like the reflection.

The purpose of an audit is to provide independent assurance that an organization's management, governance and processes are operating effectively, and that any associated assets are being properly and professionally managed.

An audit is the process of gathering and discussing information from multiple and diverse sources in order to develop a deep understanding of the current situation.

An audit is also a systematic and independent examination of various documents of an organization to ascertain how far any statements being made present a true and fair view of the reality. An audit is the process of checking that the way an organization presents information about its position is true and fair.

For smaller organizations, the audit may be conducted across the entire organization in one go.

However, for larger organizations, it makes sense to divide the trade secret audit into smaller parts rather than trying to audit the entire organization in one go.

A smart approach for conducting a trade secret audit is to begin in one area of the organization, conduct the audit there and learn from that exercise before expanding outward to other functions. There are several good options about where to start, and the selection depends on the needs of the company involved.

A company could start with a business unit, or a particular product line, or its R&D lab, or the marketing department, or its manufacturing function. If there is a section of the company that is believed to contain valuable trade secrets then the company may decide to start there.

Alternatively, a company could start with a particular class or category of trade secrets. For example, given the rise of open innovation, a company could start by enumerating those trade secrets that have been entrusted to third parties. These are often viewed as the most vulnerable trade secrets.

There are a number of ways to intelligently select a good starting point. Some of the factors are company specific, of course.

My company has conducted a number of IP audit exercises for clients. We typically divide such projects into the following phases:

Planning phase - A comprehensive plan is discussed and agreed with the client

Communication phase - Details of the project are communicated to those impacted

Interviews of key individuals phase - A series of interviews of key individuals are conducted

Data gathering phase - Various trade secret related documents are gathered from the client – including those specific to trade secrets (e.g. trade secret policy, process description, protection mechanisms, etc.) and those whose connection may not be immediately obvious but is in fact fundamental (e.g., key employment agreements, HR policies, IT policies, etc.)

Data analysis phase - All of the data gathered from the interviews conducted as well as the documents gathered is analyzed

Reporting phase - A report on the findings as well as recommendations is prepared and presented to the client

Wrap-up phase - Any outstanding issues on the project are addressed

I suggest that there are three component parts to a proper and professional trade secret audit, namely:

- Audit of the trade secret policies & procedures
- Audit of the trade secret portfolio
- Audit of the associated costs & valuations

The purpose of the first part of the audit is to sanity check if the corporate trade secret policy, procedures, processes and systems, education and governance are robust and fit for purpose and if not what enhancements need to be made.

The purpose of the second part of the audit is to examine each trade secret and the associated metadata, and determine if the trade secret warrants still being maintained as a trade secret, and if so, does it still meet the criteria to be defined as a trade secret. In order to conduct this part of the audit, having trade secret metadata is key. Trade secret metadata summarizes basic information about the trade secret, which can make finding and working with this unique form of IP much easier.

In the third part of the audit, the focus is on the costs and valuation of the trade secrets. However, it goes beyond this and should, for example, address any tax related issues.

Having a good robust fit for purpose trade secret asset management solution supports the trade secret audit process in numerous ways, such as:

- It gives tremendous structure to our audit process
- It allows data gathered during the audit exercise to be logged efficiently and effectively
- It assists greatly in the data analysis phase of the audit
- It enables much insightful reports to be generated

As the emphasis is on trade secret metadata rather than the trade secrets themselves, it allows the secrecy of such information to be maintained

It is crucial that a trade secret audit is conducted from time to time.

Companies generally gain tremendous value by taking a proactive, systematic approach to assessing their trade secrets in a comprehensive manner as described above.

A proper trade secret audit should involve the right people with business, technical and legal skills and competencies, knowledge and experience, given the unique nature of IP.

The findings of any trade secret IP audit should be reported to and discussed with senior management in the organization, given that trade secrets may be the most valuable assets the organization possesses.

Another crucial aspect of trade secret asset management is some system or tool to underpin the process.

I suggest to consider such a system or tool as being like an online library catalogue system, a register of all bibliographic items (including author's name, book title, and even approximate location) found in a library.

The catalogue is organized and indexed so that you can search by a variety of fields/indexes.

Cataloguing is the process of creating metadata representing information resources, such as books, sound recordings, moving images, etc. Cataloguing provides information such as creator names, titles, and subject terms that describe resources, typically through the creation of bibliographic records. The records serve as surrogates for the stored information resources.

Libraries have made use of catalogues in some form since ancient times. It was the growth in libraries after the invention of movable-type printing and the widespread availability of paper that created the necessity for a catalogue that organized the library's materials so that they could be found through the catalogue rather than by 'walking around'.

Putting it simply we rely on library catalogues to know what is available, and where.

The same applies to Trade Secret Asset Management.

With the passage of the Defend Trade Secrets Act in the US back in early 2016, the EU Directive on Trade Secrets due to be enacted by EU member states by 9 June 2018, and OECD BEPS guidelines including trade secrets as one form of intangible asset, this is now becoming an important aspect of intellectual property management.

Trade secret metadata summarizes information about the trade secret, which can make finding and working with this unique form of IP much easier.

Trade secret metadata may include such data as:

- The name or title of the trade secret
- The date that trade secret was created
- The person or persons who created the trade secret
- The physical location of the trade secret
- The legal owner of the trade secret
- The person or persons responsible for managing the trade secret
- The type of trade secret (technical, operational, process, financial, etc.)
- The persons with authorized access to the trade secret
- The value of the trade secret to the business
- The protection mechanisms in place to protect the trade secrets
- Whether the trade secret has been shared with a 3rd party or not
- The expiration date of the trade secret (if applicable)

I have identified over a hundred individual pieces of metadata associated with a trade secret and I continue to identify additional useful data points. It should also be noted that trade secret metadata will change over time so it is imperative that historical metadata is maintained and that there is an audit trail.

The growing importance of trade secrets has created the necessity for organisations to embrace a trade secret 'catalogue' to capture trade secret metadata and help organisations to better manage these valuable assets.

The days of just 'walking around' are over.

Trade secret asset management:

Simply deciding to keep something secret is not sufficient. Trade secret asset management involves the following:

- Education of employees about trade secrets
- Robust fit for purpose trade secret policies and procedures
- Access & access controls
- Protection mechanisms (ideally a mix of administrative, legal and technical protection mechanisms)
- Trade secrets handled properly in all agreements & contracts
- A trade secret asset management system or tool to underpin the process
- Trade secret metadata

- Trade secret valuation and costs properly managed
- Trade secret governance

The first and last items listed, namely education and governance, are like book-ends keeping everything else in order.

Trade secret meta data is the backbone of what makes trade secret management work, and we'll discuss this in more detail in the next video.