“The Management of Trade Secrets and their Risks in Commercial Exploitation”

Donal O’Connell

IPAN event, 30 Jan 2019

London

Imagine owning a property empire

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.

- 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.
- Etc.

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.

The neglected step-child of IP:

Trade secrets have in general being ignored by the IP community

- Overlooked in most IP training sessions.
- In-house IP - ‘Not part of my job spec’.
- Full service IP Firms – not listed in 'areas of expertise'.
- Not considered ‘real’ IP by many as it is not a registered form of IP

Forces at play:

Trade secrets are clearly growing in importance.

First, the law is changing:

- The Defend Trade Secrets Act was passed in the USA in May 2016.
- The EU Directive on Trade Secrets will be enacted by member states on June 9, 2018.
- China updated their Anti Unfair Competition Law at the beginning of 2018.

Second, changes in eligibility requirements and enforcement mechanisms in patent laws around the world, but especially those in the Unites States — and especially as they relate to software and business methods — make trade secrets an attractive mechanism to protect a company’s competitive advantages.

Third, with the increased use of cloud-based and licensing-based business models, across multiple industries, many businesses prefer a “black box” approach to the company’s technology more suitable to trade secrets than the disclosure-in-exchange-for-limited-monopoly approach of patents.

Fourth, cyber-criminals — whether competitors or State actors — are working overtime trying to steal trade secrets from organizations.

Fifth, more and more companies are embracing open innovation models, which necessarily requires sharing and collaborating on trade secrets with others.

Sixth, changes in employment models are leading to a highly mobile and transitory workforce where companies now have increased risk that their employees will walk out the door with their valuable trade secrets.

Seventh, there is growing interest in trade secrets by the tax authorities:

- OECD BEPS Guidelines now include trade secrets as an intangible asset requiring proper management.
- Much of the EU's Anti Tax Avoidance Directive (ATAD) enacted on 1 January 2019 relates to intangibles including trade secrets
- Patent Box Tax Regimes in a number of jurisdictions are now allowing trade secrets as qualifying IP.
- The US Government is encouraging US companies to repatriate their IP back to the US by lowering tax rates for royalties received from all forms of IP to be materially less than the rate on ordinary corporate income.

Eighth, trade wars are linked by some to trade secret theft concerns.

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

Definition:

Let's go back to the basics. A trade secret is any information that:

- is secret.
- has value.
- is reasonably protected.

Broadly speaking, any confidential business information which provides an enterprise a competitive edge may be considered a trade secret.

Contrary to popular belief — especially among business owners — trade secrets are not only found in top secret, highly-secure research labs. Rather, almost every business possesses trade secrets, regardless of the size and industry focus of the business.

Current state analysis:

Unfortunately, many companies are poor when it comes to trade secret asset management.

Executives from companies of all types acknowledge the importance of trade secrets to their businesses while privately admitting that their company has no idea how many trade secrets they have, which ones are important, or how any of them are protected. The same executives will also sheepishly admit that they have no idea how many trade secrets their company has received from third parties in various business ventures, how adequately their company protects them, or if they even bother to return or destroy them once the collaboration ends.

- Trade secrets are poorly managed
- Education is not happening
- 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 information sharing between the legal / IP function and the Accounts / Tax function
- There is no audit trail.
- No governance

Nearly everyone acknowledges the importance of trade secrets while doing very little to protect them or even making a simple list. It's like knowing you have a Rembrandt in your attic and not bothering to have it appraised, insured, or even protected from rodents and birds.

Good practice:

Those exceptional companies who have this mastered tend to have the following things in place

- Education of employees about trade secrets
- A robust trade secret policy
- Fit for purpose trade secret process & procedures
- A system to underpin that process
- Good quality trade secret metadata
- Trade secret governance

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.

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

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

If a company only has one or two trade secrets, then they probably do not require any trade secret asset management system. However, if the number of trade secrets in a company is more than a handful; if they are sharing their trade secrets with others; if other entities are entrusting their trade secrets to the company; if the company has any direct or indirect links with entities in the US (given the growing issue with trade secret litigation there); if the company has trade secrets located across diverse EU member states (given the EU Directive on Trade Secrets being enacted in June 2018), if the company is doing any business in China (for the reasons outlined in this paper); and/or if the company is conducting any IP due diligence exercises due to some corporate event (e.g. M&A, JV, Investment Round, etc.), then a trade secret asset management system is absolutely required.

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’. 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.

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 organization.

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

I would argue that trade secret metadata is key. Without trade secret data, you have no trade secret information. Without trade secret information, you have no trade secret knowledge.

The challenges with keeping something secret:

Deciding to keep such assets secret is however easier said than done. It may seem like a very good idea and there may be common agreement to keep such assets secret, but it is often extremely difficult to do so in practice

- Human nature
- Openness
- Digitization of information
- Organizational loyalty
- Cyber crime
- Lack of processes to manage secrets

The risks associated with trade secrets:

Trade secrets can be extremely valuable, perhaps the most valuable assets an organization possesses. However, trade secrets by their very nature are somewhat fragile. They face a variety of risks which need to be mitigated.

- Some risks relate to the information itself
- Some relate to how the information is documented
- Some relate to access, access controls and protection mechanisms

- Some related to the independent actions of 3rd parties
- Some relate to the trade secret being misappropriated
- Some relate to legal or regulatory requirements to publish the information
- Some relate to the sharing of trade secrets with other entities
- Some relate to being entrusted with the trade secrets legally belonging to others
- Some relate to trade secret asset management and the associated policies, processes and systems.

Sharing trade secrets with others:

When sharing your trade secrets with others, just remember that NDAs are like confetti.

When English poet John Donne wrote his famous line “No man is an island,” almost 400 years ago, in many ways he was forecasting the future of business as it operates today. No company is an island. It interacts with many other entities.

In many of these business relationships, the companies involved will pass trade secrets back and forth.

Ideally, whatever legal framework is put in place should contain details of the standard by which the parties involved will handle the disclosed trade secrets provided to them by the other party. However, this is an aspect that is often overlooked by many companies.

Basically, Party A divulges trade secrets to Party B which Party B then is expected to look after, care for and protect. However, Party A often fails to ask Party B to explain their overall process for managing trade secrets and specifically how Party B will actually care for the trade secrets entrusted to them by Party A.

One simple question Party A should ask of Party B is for details on how Party B look after its own trade secrets. Perhaps it should delve a little deeper and ask a series of questions…

Q1/ Does the other party have a trade secret **policy and associated procedures** and does it extend to trade secrets entrusted to it by others?

Q2/ Does the other party provide **education** for its employees about the handling of trade secrets?

Q3/ How does the other party handle **access and access control** procedures to limit the number of people having access to trade secrets, including trade secrets entrusted to it by others?

Q4/ What are the various **protection mechanisms** the other party has in place to protect trade secrets, including trade secrets entrusted t it by others?

Q5/ Does the other party conduct any regular **audits** of its process to handle trade secrets and if so how are these actually conducted? What were the key findings from the last such audit conducted?

Q6/ Does the other party have a **system or tool** in use to underpin its process for handling trade secrets, including those trade secrets entrusted to it by others?

Q7/ What **governance** structure and process does the other party have in place regarding trade secret asset management?

The ability to ask the right question is more than half the battle of finding the answer.

Of course, asking these questions is only half the battle. Getting the answers back and satisfying yourself that these answers are a true

reflection on how the other party manages trade secrets including those trade secrets entrusted to it by others is crucial.

Final thoughts:

Companies need to understand and appreciate that deciding to keep something as a trade secret is not the end but rather the beginning of an interesting journey, and that there are a number of challenges to be overcome.

Without trade secret data, one has no trade secret information. Without trade secret information, one has not trade secret knowledge.