How to manage trade secrets

Trade secret theft and incidents

Donal O'Connell:

In this educational video on trade secrets, the issues we'll explore are:

- The typical trade secrets incidents that befall companies
- The anatomy of a trade secret misappropriation court case
- Managing the trade secrets belonging to others
- The threat from cyber criminals

Let's start straight away with the typical incidents that befall companies.

A trade secret continues for as long as the information is maintained as a trade secret. However, information may no longer be considered to be a trade secret once it becomes easily accessible, is no longer properly protected or has no commercial value.

Many organisations are failing to properly protect these valuable assets, and this failure is not unique to any one specific stage in a typical business life cycle.

Ok, now we will focus on a list of the most common trade secret incidents we see befall businesses …

- First, and especially relating to start-ups, a founding member leaves the company and takes some trade secrets with him and then establishes another competing start-up.
- The company fails to understand that certain things should be kept secret and shares too much information with an external party.
- A potential investor walks away after asking the company about their trade secret policy, processes and systems to properly protect such valuable assets.
- A disgruntled employee leaves the company and takes some trade secrets with him, put onto a memory stick on his last day of employment.
- A new starter joins the company but has stolen trade secrets from his previous employer, and shares that trade secret with his new colleagues
- A supplier entrusted with one of the trade secrets of the company shares it with a competitor.
- Cyber criminals hack the network of the company and steal some trade secrets. Cyber criminals are after the trade secrets of the company, the confidential business information which provides an enterprise with a competitive edge.
- The company divests one part of the business but mistakenly gives away some trade secrets as well.
- A collaboration partner accuses the company of stealing one its trade secrets, breaking the terms and conditions of the collaboration agreement.

I suggest that a business should strive to avoid or at the very least minimise these typically incidents from happening.

Firstly, the business needs to display management and leadership with respect to the trade secrets of the organisation.

Secondly, the organisation should embrace trade secret metadata.

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

Thirdly, it is important to note that trade secrets are fragile and require some TLC, using a combination of cultural, legal, technical and administrative means.

Trade secrets and know-how can be some of the most important assets in the intellectual property portfolio of an organization. They are at least on a par with other forms of intellectual property such as patents and trademarks. Some would argue that trade secrets and know-how are the crown jewels of any intellectual property portfolio.

Trade secret asset management:

Trade secret asset management is about the policies and procedure, processes and systems, education and governance defined and taken into use to help manage such assets.
Simply deciding to keep something secret is not sufficient!

I suggest that trade secret asset management consist of a diverse range of elements, such as:

- Having a trade secret policy in place
- Designing, developing and deploying a trade secret process within the organisation
- Taking a robust fit for purpose trade secret asset management system into use to underpin that process
- Including a section on trade secrets to the basic IP training for all employees

Trade secret asset management:

- Identifying trade secrets across the entire organisation
- Identifying any trade secrets shared with 3rd parties
- Identifying any trade secrets belonging to 3rd parties and entrusted to the company
- Putting the appropriate administrative, legal and technical protection mechanisms in place
- Gathering metadata about the trade secrets for management purposes
- Installing a culture of confidentiality within the company as far as trade secrets are concerned
- Putting a governance structure in place
-

Anatomy of a trade secret misappropriation case:

OK, let’s turn our attention to the anatomy of a trade secret misappropriation court case. Let us imagine that Company ABCD has a portfolio of IP assets, including a number of trade secrets. These trade secrets assets may be found across different functions in the organisation and include:

- Some algorithms within the R&D function
- Customer data managed by Sales & Marketing functions
- Some filtration process held by Operations in the factory
- Some negative know-how in the form of failed tests and test data held by the Test function
- Some new business plans by the Business Development function

Like many organisations, these trade secrets are of tremendous value to the company and among the most valuable intangible assets it possesses.

Stop thief !!!

Let us imagine for a moment that one of Company ABCD’s trade secrets was stolen. It may have been stolen by a former executive of the company, a disgruntled employee, a supplier, a competitor or some hacker.

Let's assume in this case that the trade secret stolen was Algorithm XYZ and that the accused is a former executive who has since joined a competitor.

Let's also assume that the alleged theft took place on 15 November 2015, a randomly selected date.

A court case then takes place some months later on 27 February 2017 involving Company ABCD and the accused.

At the court case Company ABCD has to prove three things, namely that Algorithm XYZ was a trade secret as of 15 November 2015 AND that the accused stole the trade secret AND that the theft of the trade secret caused damage to the company. Of course the accused will try to prove that Algorithm XYZ was not a trade secret as of 15 November 2015 OR that no misappropriation took place OR that no damage was caused.

Although the court case is taking place on 27 February 2017, Company ABCD must prove that Algorithm XYZ was being treated as a trade secret at the time of the alleged theft, i.e. back on 15 November 2015.

Whether Company ABCD treats Algorithm XYZ as a trade secret on 27 February 2017, the date of the court case, is irrelevant.

One could argue that there is an initial step before we even get to these three steps described above, namely discussing and agreeing what information is actually in dispute. There seems to

be a trend in trade secret disputes that at the outset of the dispute the trade secret is defined with 'reasonable particularity' prior to letting the case proper proceed.

To qualify as a trade secret, Algorithm XYZ …

- Must not be in the public domain
- Must be kept secret
- Must be documented
- Must have access limited
- Must be protected ideally using a combination of administrative, legal and technical means
- Must have value to the company now or in the future
- Must have the appropriate legal framework in place if shared with a 3rd party

Company ABCD will have to produce evidence that it was treating Algorithm XYZ as a trade secret back on 15 February 2015. Evidence is the available body of facts or information indicating whether a belief or proposition is true or valid. 'Trust me, your Honour' does not qualify as evidence.

Now, I don't know about you but I can barely remember what I did last weekend.
If Company ABCD has a trade secret process underpinned by a trade secret asset management solution with good quality trade secret metadata, then it has put itself is a strong position to be able to show the court that Algorithm XYZ was indeed being treated as a trade

For organizations of any size, it is vitally important to be able to manage and track who has access to the trade secrets of the company, how such trade secrets are protected and if they are been shared with any 3rd parties. It is also crucial to have an audit trail to capture such details back in time.

Without any such trade secret process, system and associated metadata, then proving that Algorithm XYZ was being treated as a trade secret back on 15 February 2015, never mind last weekend, becomes a major challenge.

Good quality trade secret metadata can also help the company describe the trade secret with 'reasonable particularity' without having to divulge the actual trade secret itself. I don't care how good a protective order may be, there is always an added danger of loss.
Trade secret litigation has been on the rise for a number of years and that trend is most likely to continue.

For anyone interested in delving into the details, I suggest taking a look at the 'Trends in Trade Secret Litigation Report 2017' by Stout.

At first glance, you may be somewhat perplexed by this. When and why should a company be concerned about managing trade secrets belonging to some 3rd party? It is tough enough for most companies to properly and professionally manage their own trade secrets, not to mind worrying about the trade secrets belonging to others. However, more and more, companies are

indeed facing the challenge of having to manage trade secrets belonging to others. Allow me to explain.

No company is an island:

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 may interact with universities, cooperate closely with key suppliers and vendors, collaborate with application developers, content providers, technology house and design houses, plus work with various communities including 'open’ communities, innovation networks, Standardization Setting Bodies as well as customers and end-users. It may also involve working with start-ups and venture capital funded entities. No company is an island. In most if not all of these business relationships listed above, the companies involved will pass trade secrets back and forth.

A legal framework:

A legal framework of some sort is usually put in place between the parties, with the first step usually being the signing of a Non-Disclosure Agreement (NDA). This is a relatively simple legal agreement between a company and a counter-party of that company to exchange information, for the purpose of a project, marketing campaign, R&D or sourcing, etc. Examples of information which can be protected by a NDA are business proposals, financial data, new ideas, etc. Under an NDA, the signer promises the recipient that he will not disclose certain information to any third parties, except under circumstances described within that contract. Although NDAs are specifically mentioned here, this legal framework may include a Memorandum of Understanding, a Development Agreement, a Commercial Agreement and more.

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.

Good practice:

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…

- Does Party B have a trade secret policy and associated procedures?
- Does Party B provide education for its employees about the handling of trade secrets?
- How does Party B handle access and access control procedures to limit the number of people having access to trade secrets?

- What are the various protection mechanisms Party B has in place to protect trade secrets? Do these protection mechanisms include administrative, technical and legal measures?
- Does party B conduct any regular audits of its process to handle trade secrets and if so how are these actually conducted?
- Does Party B have a system or tool in use to underpin its process for handling trade secrets?
-

Of course Party B if it is providing trade secrets to Party A should ask these exact same questions of Party A.

Final thoughts:

In today's competitive market, companies need to be as innovative as possible to prosper in the business environment and to keep pace with progress. No company can achieve this in isolation. Instead the company must cooperate and collaborate with others.

To this end, the development and acquisition of useful information, some of it qualifying as trade secrets, is crucial to create and provide new and improved goods and services. Information about technology that makes a company's product unique, prototypes, or a list of key clients or customers are just a few examples of such trade secrets. As many of these trade secrets can be of great commercial value and be of significant importance to the company concerned, its uncontrolled disclosure may potentially lead to serious consequences.

Given some of these trade secrets will be shared with others, it is therefore imperative that these others fully respect this information, and strive to keep this valuable information confidential. If such trade secrets are not properly respected, it may cause damage to the reputation of the company, adversely impact key business relationships and even cause the company to end up being sued in court.

Making money from cybercrime:

A growing source of income for the cyber criminals is generated from the theft of such corporate trade secrets.

Theft of trade secrets means the theft of ideas, plans, methods, processes, technologies, data or any sensitive information.

These secrets are owned by the company and give it a competitive edge. Theft of trade secrets damages the competitive edge and therefore the economic base of a business.
Trade secrets are plans for a more advanced computer, designs for a more fuel-efficient engine, a company's new manufacturing process, supplier agreements, user data, etc. etc. Trade secrets exist in almost all companies across all industry sectors, and many trade secrets are extremely valuable indeed.

Three years ago, the Wall Street Journal estimated that the cost of cyber-crime in the USA alone was approximately $100 billion. In 2015, the British insurance company Lloyd's estimated that cyber-crime cost companies as much as $400 billion a year.

The World Economic Forum (WEF) said that a significant portion of cyber-crime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot.

The spy agencies here in the UK believe that industry networks are targeted by sophisticated cyber espionage attacks on an almost continuous basis, with many of these attacks being suspected of being state-sponsored. The head of cyber for MI5 in the UK has said that having a foreign spy agency attack your business system is now as certain as "death and taxes". The cyber criminals are after any trade secrets that can be harvested and monetized. They are not seeking to steal what is on the menu in the company canteen. They do not want to know what colour paint is on the wall of the offices of the CEO. They are not after information which has already been put into the public domain by the company. Rather, these cyber criminals are after the trade secrets of the company, the confidential business information which provides an enterprise with a competitive edge.

How the cyber criminals attack:

The cyber criminals leverage a variety of different approaches and techniques to identify the vulnerabilities in the IT network of the company and then attack.

The cyber criminals may leverage backdoors into the IT network. They may try a denial-of-service attack or even a direct-access attack. They may try eavesdropping, spoofing, and even tampering directly with the IT network of the company. The cyber criminals may use privilege escalation, phishing, clickjacking or social engineering techniques. In some cases, they create a false environment of stealing non-pertinent data, diverting the attention of incident responders only to exfiltrate trade secret data residing elsewhere on the network. Regardless of what, where and how they attack, they are after the trade secrets of the company.

Trade secrets within companies:

Given that the cyber criminals are after a company's trade secrets, one would expect to see mature and sophisticated trade secret management practices deployed by most companies. However, this is not the case.

The typical findings within companies are that:

- Knowledge of trade secret legislation is limited.
- Companies are not properly managing their trade secrets with no clear ownership of the trade secret management process or the secrets themselves.
- Documentation about the trade secrets is often poor.
- Access to and access control around its trade secrets is very ad hoc.

- Protection mechanisms (administrative, legal and technical) deployed to safe-guard its trade secrets is poor or non-existent.
- There is a lack of any classification of the trade secrets by the company.
- Details on whether trade secrets has already been shared with 3rd parties was often missing
- Information of any trade secrets belonging to 3rd parties but entrusted to the company is scarce.
- There is often no audit trail.

If the cyber criminals are to be stopped from stealing the trade secrets within companies, it requires that the IT folks and the Legal & IP folks work together as both advanced computer and network security as well as proper trade secret asset management are required.

“If you knew which horses were the thoroughbreds, you wouldn’t have to guard the entire herd” - Rich Weyand, The Trade Secret Office Inc.

The next video will go into more depth on the subject of managing trade secrets, with more advice and practical guidance.