

# How to manage trade secrets

## What is a trade secret? Part I

*Welcome to the Academy by PatSnap course on How to Manage Trade Secrets. My name is Duncan Clark and I am Head of IP Education here at PatSnap. For this course, we are delighted to be joined by Donal O'Connell, Adjunct Professor of IP at Imperial College Business School in London and member of global IP strategist group IAM300.*

*In this series of videos, Donal will be navigating us through the complex world of trade secrets. This is the first part in a two-part series of videos on the definition of a trade secret.*

### **Donal O'Connell:**

In terms of trade secrets, as a starting point, there are three main aspects to bear in mind... A trade secret is defined as any information that is:

First, not generally known to the relevant business circles or to the public. The information should also not be readily accessible.

Second, it confers some sort of economic benefit on its owner. This benefit must derive specifically from the fact that it is not generally known, and not just from the value of the information itself. It must have commercial value because it is a secret. Commercial value encompasses potential as well as actual value.

And finally, point three: It must have been subject to reasonable steps by the rightful holder of the information to keep it secret. What is reasonable can vary depending on the specific circumstances.

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.

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

With those points in mind, in this video, I plan to delve deeper into specific aspects of this definition of trade secrets, and we'll do that in the following manner:

In the first section, to gain context, we will compare and contrast trade secrets with some other forms of IP

Then, we'll explore some of the challenges with keeping such information secret

Let's start with trade secrets versus confidential information...

Broadly speaking, any confidential business information which provides an enterprise a competitive edge may be considered a trade secret. However, not all confidential information within an organization qualifies as a trade secret.

Within an organization, there will be multiple levels of confidential information, with trade secrets being at the highest level of confidential information.

“A distinction should be drawn between widely accessible (internal) confidential information and trade secrets which require special governance. This means that the normal processes to manage confidential information may not be considered adequate for managing trade secrets.” Although the terms confidential information and trade secrets as well as proprietary information and even know-how are often used interchangeably, these terms are interpreted differently and the remedies for the unauthorized revelation of such information may also differ.

So although there is substantial overlap between trade secrets and confidential information, they are in fact different things.

### **So, what qualifies as a trade secret?**

“A trade secret can be a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information which is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers.”

The subject matter of trade secrets is defined in very broad terms and includes sales methods, distribution methods, consumer profiles, marketing plans, supplier lists, client details, and manufacturing processes. Trade secrets may encompass manufacturing or industrial secrets and commercial secrets.

Trade secrets may exist in any of the three key business dimensions of operational excellence, customer intimacy and product leadership.

Generally speaking, any confidential business information which provides a business with a competitive edge may be considered as a trade secret.

Trade secrets can even protect negative know-how, for example the results of failed experiments. Negative know-how is essentially what does not work. Negative know-how can include details of previously attempted, but flawed techniques or 'blind alleys' that did not achieve their intended results. The biggest misperception people have about failure is that it is all bad. But from an engineer's point of view, a failure can contain all sorts of really useful information.

“Ever tried. Ever failed. No matter. Try again. Fail again. Fail better.” - Samuel Beckett  
Understanding what does not work is just as important as understanding what does.

The inherent proprietary value of know-how lies embedded in the legal protection afforded to trade secrets in law. A trade secret is virtually anything that is secret, and that imparts value to its holder as a consequence of that very secrecy.

So trade secret laws protect know-how. Interestingly trade secret laws also protect negative know how.

A final determination of what information constitutes a trade secret will depend on the circumstances of each individual case, but it is clear that the subject matter is very broad indeed.

Perhaps the most famous trade secret is the Coca-Cola formula reputedly stored in a vault in the city of Atlanta. Google's proprietary search algorithm; KFC's blend of eleven herbs and spices; and the compound WD-40 (that distinctive spray with thousands of uses) are other famous examples of trade secrets.

### **Trade secrets involved in recent court cases:**

It is worthwhile to take a few moments to analyse the trade secrets involved in some recent trade secret misappropriation court cases and includes...

- hotel search and reservation data
- wireless technology
- recipes
- production process information
- data analytics
- driverless car technology
- earth moving equipment
- drug marketing and pricing information
- flexographic printing plate technology
- wearable technology business plans
- financial software code and algorithms
- software for healthcare
- medical device technology
- executive search
- product test robot
- USB technology
- business information
- engineering drawings
- quality control procedures
- internet beaming balloon technology
- agreements and contracts
- financial models
- sales leads
- customer lists

- marketing and sales strategies
- swimming pool marketing material
- cost and pricing information
- biotech heart valve designs
- confidential bid information
- software code for trading systems
- data transfer technology
- online eyeglass prescription test information

As stated earlier, any confidential business information which provides a business with a competitive edge may be considered as a trade secret.

Comparing and contrasting patents and trade secrets:

Patents and trade secrets represent two of the most common methods to protect creativity and innovation.

Trade secret protection has the advantage of not being limited in time, and may continue indefinitely as long as the secret is not revealed to the public. Patents last in general for up to 20 years. Trade secrets have immediate effect whereas patents have to be drafted, filed and prosecuted which takes a few years on average. Trade secret protection does not require compliance with formalities such as disclosure of the information to a Government authority. The scope of trade secrets is virtually unlimited which is not the case for patents. Trade secrets involve no registration costs unlike patents, although there may be some costs related to keeping the information confidential.

However, if the trade secret is embodied in an innovative software product or service, then others may be able to inspect it and ‘reverse engineer’ it to discover the trade secret and be thereafter entitled to use it. However, independent invention is no defence against patent infringement. A trade secret has traditionally been more difficult to enforce than a patent, but that has changed dramatically in recent times, and I would now argue that there is very little difference in this regard.

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. Let’s now look at some of the reasons why...

#### **Human nature:**

Firstly, human nature...

Some people just find it difficult to keep a secret. One sometimes hears people say ...  
 “I’ve been sitting on a really awesome secret the past couple of days, and I have to say, it’s killing me that I can’t tell anyone.”

Keeping something secret requires both self control and the ability to make choices, but withholding information creates stress for some people and can leave them feeling alone and

alienated from those that don't know. This can evoke a lot of anxiety which makes it more difficult to think clearly, and for people who find it hard to manage those feelings or who are very anxious, keeping a secret can be almost impossible.

Some research has shown that blabbing secrets may have less to do with a person's need to share salacious gossip and more to do with how their brain works.

### **Openness:**

Next, openness...

Openness is an overarching concept or philosophy that is characterized by an emphasis on transparency and free, unrestricted access to knowledge and information, as well as collaborative or cooperative management and decision-making rather than a central authority.

Openness can be said to be the opposite of secrecy. Many companies are embracing this spirit of openness.

Traditionally, internal innovation was the paradigm under which most firms operated, with most innovative companies keeping their discoveries highly secret and no attempt made to assimilate information from outside their own research and development laboratories. This was driven by the belief that: "the smart people in our field work for us". However, in recent years the world has seen major advances in technology and society which have facilitated the diffusion of information. Companies have also begun to realise that "not all the smart people work for us and that we need to work with smart people inside and outside our company". Such collaboration can take many forms, from working with universities, cooperating closely with key suppliers and vendors, collaborating with application developers, content providers, technology house and design houses, plus working with various communities including 'open' communities, innovation networks, standardisation bodies as well as customers and end-users. It can also involve working with start-ups and venture capital funded entities, as some of the smallest companies can achieve great things with limited funding.

### **Digitization:**

OK, digitization. The business world is going digital. This of course means different things to different companies.

Fundamentally, digitization means converting data from analog formats into digital formats, but it means much more than this. Companies are moving to paperless environments converting their papers and files into digital formats. Key business applications are being computerized. Companies are taking their manual or offline activities or processes and converting them to online, networked, computer-supported processes.

Regardless of what digitization means to a particular company, it generally promotes easy discovery, access, and use of information.

### **Organizational loyalty:**

Then, there's organisational loyalty – organizational loyalty is a general term and denotes a person's commitment and attachment to the place they work.

Long gone are the days when an employee joined a company after leaving school and stayed with that company until retiring. These days, people expect to move around across numerous companies over their working career.

The generation of young millennials now in the work place clearly have a different set of expectations compared to older generations about their careers. In a nomadic world, one of the casualties is a decreasing sense of loyalty to a particular organization. If loyalty is defined as being faithful to a company, then there seems to be a certain amount of disloyalty in the workplace these days.

The recent global recession has also had an adverse impact on such loyalty as loyalty is a two way street.

### **Cyber crime:**

Cyber crime, now. Cyber attacks are crimes in which the computer system of the company is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage. Cyber theft comprises crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data. Other computer security incidents encompass spyware, adware, hacking, phishing, spoofing, ping, port scanning, and theft of other information, regardless of whether the breach was successful. This is a growing problem for all companies. Cybercrime is one of the greatest threats facing any company, and has enormous implications for its security, prosperity, and safety. The range of threats and the challenges they present for companies is expanding just as rapidly as technology evolves.

### **No process in place to manage such secrets:**

And lastly, no process in place to manage such secrets.

Many companies lack a robust fit for purpose process to manage such secrets.

A process is an interrelated set of activities designed to transform inputs into outputs, which should accomplish your pre-defined business objectives. Processes produce an output of value, they very often span across organisational and functional boundaries and they exist whether you choose to document them or not.

A process can be seen as an agreement to do certain things in a certain way and the larger your organisation, the greater the need for agreements on ways of working. Processes are the memory of your organisation, and without them a lot of effort can be wasted by starting every procedure and process from scratch each time and possibly repeating the same mistakes.