IP Risk and IP Risk Management

What are typical IP related risks?

Introduction

Hello and welcome to the Academy by PatSnap course on IP Risk. We're delighted to welcome our partners and experts in this field, Chawton Innovation Services, who will be guiding us through the complex environment of risk and how that relates to intellectual property. I'm happy to introduce Donal O'Connell, Managing Director of Chawton Innovation Services, who will be our host for this session. In this module, we'll start by considering the typical IP risks. So let's join Donal now and begin with IP value and risk:

Donal O'Connell

Any business professor will tell you that the value of companies has been shifting markedly from tangible assets, "bricks and mortar", to intangible assets like intellectual property in recent years. Research has indicated that intangibles now account for between 60% and 90% of the total value, depending on the industry sector.

There is no data available on the scale of the risks associated with IP but one can assume that it is significant, and probably around this 60% to 90% mark. There is indeed some data available on the size of the problem associated with certain specific types of IP related risks such as counterfeit goods, patent litigation, trademark disputes, data hacking and so forth. So what do we mean by risk and what do some of these IP related risks look like?

Risk is the chance of something going wrong, and the danger that damage or loss will occur. By its very nature, there are both rewards and risks associated with IP. For anyone involved in IP, then IP related risks are part of working life.

Not all IP related risks are the same and they may be broken down into a variety of different categories, such as the form of IP involved (for example patents, trademarks, copyright, trade secrets, and so forth); the impact and probability of the risk; the source or origin of the IP related risk; the date when the risk is likely to materialise; the IP activity impacted; the geographical nature of the IP risk; whether they are generic or specific in nature; the group or sub-group most impacted by this risk in the organisation; amongst other factors.

Any company faces a variety of IP related risks, some foreseen others unforeseen. I have yet to meet a company who does not have one or more IP related risks to consider.

However, many ignore the risks associated with IP or only react when the risk has materialised, which is most times too late. Also, many of the IP related risks that companies face are due to their own lack of awareness or proper understanding of IP, and/or their own actions or lack of actions.

IP litigation is a threat to all businesses, large and small but it is by far not the only form of IP related risk. There are indeed many different types of IP related risks that a company may face. The bottom line is that IP related risks are a significant issue for many companies. With so much value encapsulated in intangibles it is a fiduciary duty for directors to have clear understanding of IP risks and plans in place to offset those risks

Ok, so what is the source of IP related risks?

Now, a significant percentage of the IP related risks that an organization faces originates within the organization itself due to the activities of its own people. Sometimes it is due to a lack of awareness and education of IP by employees, other times it is a deliberate act.

In recent years the world has seen major advances in technology and society which have facilitated the diffusion of information, and companies now work with people inside and outside of the organization. However, many IP risks originate from these very same entities within the eco system of a company, namely its suppliers, partners, distributors, customers and even end-users. Some entities within the eco system of a company just may not treat the company's IP or the IP of 3rd parties with the proper attention and respect it deserves, resulting in IP related risks to the company.

IP related risks posed by competitors tend to get most press attention. Given the very nature of IP and the legal rights associated with it, IP assets belonging to competitors who are designing, developing, manufacturing, distributing and/or selling similar products or services, pose a potential IP risk to any company.

IP related risks may originate from entities like IP holding companies, patent assertion entities, and non-practicing entities (NPEs) plus others. Recent US patent statistics show that patent litigation, driven by such type entities, is significant. Although primarily focus on patents and centred in the US, IP related risks coming from independent 3rd parties is not limited to that particular form of IP or to that particular jurisdiction.

IP relates risks may come from the activities of Government Departments, Industry Regulators, Inter-Operability Standards Setting Bodies, and of course Intellectual Property Offices themselves. IP changes taking place in some key jurisdictions may pose a risk to some. Some companies will clearly benefit from these reforms but others may find their IP risk profile changes in an adverse manner.

Illegal entities like hackers and counterfeiters pose major IP risks to many companies. Hackers are generally external individuals, criminal gangs or even Government sponsored entities whose sole objective is to gain illegal access to the company's computer infrastructure, with the intention of committing a crime such as the theft of confidential information or trade secrets. Counterfeit goods can include fake designer clothes, bags, watches, accessories and perfumes as well as pirate DVDs, CDs, smartphones and computer games. They can also include medicines and components of automobiles and aircraft. The size of the problem posed by counterfeiters is staggering.

Involving an external IP Firm or IP Service Provider into a company's IP operations basically means buying certain work results from third parties. Subcontracting to an external entity is not always easy. Yes it can bring tremendous value but it can also bring risks.

Examples of IP related risks:

We will now explore highlight some examples of IP related risks, focusing on:

- patent related risks
- trade secret related risks
- soft IP related risks
- open source software related risks

Let's start, then, with patent related risks:

Many companies fail to keep in mind that a patent does not give them the right to make its invention. Rather it gives a company the right to stop others from making its invention.

A patent is an exclusive right granted for an invention. Patent protection means that the invention cannot be made, used, distributed or sold without the patent owner's consent. The owner of a patent has the right to decide who may or may not use the patented invention.
If a company is built on technology of any kind, being called out for infringing an existing patent held by another company could easily see its investment in research and development wasted. But while technology is central to most patent disputes, it's not just technology companies that are at risk of infringing patents in the ever more competitive scramble to be innovative.
There are currently about 10 million active patents in existence, and these patents cover a diverse range of technologies and geographical locations.

Of course, there are also risks associated with a company's own patenting activities. The simplest risk that a company takes if it files a patent for its invention is that it won't get one. Not every filing results in a patent. There is also the risk that the time and energy spent in obtaining a patent won't pay off. Inventors don't work in a vacuum. The same problem that inspired the company to create its invention might have led some other company to the same solution independently.

If the company engages in patent licensing activities, then it should be aware of the associated risks., If a company engages in IP licensing, then it is most important to properly manage and maintain these agreements. A recent audit case of some long-standing patent and know-how licences highlighted that almost every single licensee was in breach of its terms: either the fees being paid, when they were paid, how they were calculated, interpretation of what constituted Licensed Products(!), territories included, no reports, or …worse still… all of the above!

Ok, next, trade secret related risks:

A trade secret is defined as any information that is:

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

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

Here's a list that captures some of the typical trade secret incidents we see befall businesses …

- 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 dis-grunted 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.
- 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.

Next up, soft IP related risks:

There are multiple forms of IP such as patents, trademarks, copyright, etc. etc.

The term ‘soft IP’ is sometimes used to refer to trademarks, copyright, and domain names, in contrast to ‘hard IP’, which is sometimes used to refer to patents.

I accept that use of this phrase is controversial among some IP practitioners, and that the term soft IP may mean slightly different things from one IP practitioner to another
Here, I focus on soft IP and in particular on trademarks, domain names and social media handles, and some of the common mistakes made by companies, particularly SMEs, as far as these forms of IP are concerned.

Some companies are simply confused between having registered their company at Companies House and registered a trademark and a domain name. Registering the company name at Companies House provides no IP protection. Just for reference, Companies House is the UK’s registrar of companies and is an executive agency and trading fund of the UK Government.
Some companies are confused between registering a trademark at the Trademark Office and registering a domain name with some domain name registrar. A domain name registrar is an organization or commercial entity that manages the reservation of Internet domain names. Such registrars have absolutely no involvement with trademarks registration.

Some companies select a brand name without considering how easy it will be to protect. Calling a business, product or service a commonly used word such as ‘Apple’ is going to be much harder to protect than a name like ‘Adidas’ because Adidas is a made up word.
The recent introduction of new generic Top Level Domains (gTLDs) represents one of the biggest changes to the Internet since its inception. It provides opportunities for companies and brand holders to re-energize their online domain name strategies, but it also poses some risks if companies fail to act. It is interesting to see what many banks have done. Many banks and financial services firms acquired their own dot brand new gTLDs to enhance stability, increase security and reduce phishing attacks - .Barclays; .HSBC; .AIG to name but a few.

A number of companies have selected names for their products or services which were not identical but were very similar to existing brands. They mistakenly thought that because there were not 100% identical, that this would not be a problem.

A significant number of companies fail to register domain names and trademarks in foreign countries, and in countries they actually planned to enter in the short to medium term. The risk of course is that competition or a local business will register the name instead and so makes defending rights more costly. One of the most common misconceptions about trademark rights is the notion that one automatically accrues rights abroad, when in fact trademarks are "territorial" in nature. "Territorial" rights apply, rather intuitively, only within the borders of the country where they are obtained.

Many companies fail to register their trademarks with Customs. Counterfeit goods can include fake designer clothes, bags, watches, accessories and perfumes as well as pirate DVDs, CDs, smartphones and computer games. They can also include medicines and components of automobiles and aircraft.

The size of the problem posed by counterfeiters is staggering. To help stop counterfeit products crossing borders, it is strongly advised to register your trademark with Customs, and to have a regular training program in place with them.

Consumers increasingly rely on social media, irrespective of how they make the actual purchase: via clicks, bricks, or a mix. Retailers and brand-builders cannot overlook this phenomenon and clearly many brands have now embraced this social media world in one way or another. More and more brands are working to optimize their online presence, protect their brand equity and drive profitable e-commerce sales growth. Today launching a company, product or service without an associated Twitter, Facebook or Instagram account being available can make communication with the target audience very challenging.

We have seen a number of companies and their marketing folks comes up with some great product names, and produce some great marketing literature, only for them to then discover that somebody else already had the name registered in one of the major countries the SME was planning to enter. A simple search would have avoided such problems.
Some companies have indeed conducted availability checks on names but had failed to conduct any foreign language checks. So the selected names were available in English but the companies faced challenges with key foreign languages.

It is the responsibility of the trademark owner to protect their brand. It is therefore important to have at least minimum services in place to identify infringements.

Many companies do not consider defensive domain name registrations. This involves considering variations on a trademark that might be used by a cyber squatter. For example it might be worthwhile to register both Apple.com and Apples.com to avoid costly UDRP cases in order to recover the name.

IP insurance was not on the radar of many companies. There can be advantages in taking out IP insurance to defend against other companies taking action because of a perceived trademark infringement.

And finally, open source software related risks:

Open-source software is computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.

"Source code" is the part of software that most computer users do not ever see. It is the code computer programmers can manipulate to change how a piece of software - a "program" or "application" - works.

Although embracing open source software can bring tremendous benefits, a company may also face a diverse range of issues associated with open source software which will all need to be properly and professionally managed. Like many things in life, there is both value and risk associated with open source software.

A number of IP issues can arise when companies embrace open source software, such as with copyright and patent related matters.

Companies have indeed faced copyright infringement issues when embracing open source software. A major IC company's BSD (Berkeley Software Distribution) license's breached copyright in one of its products due to non-disclosure of license information. A major Consumer Electronics company's public license breached copyright in one of its products because of non-disclosure of license information.

Companies often run into copyright issues when embracing open source software, often forgetting to do the basics. Companies fail to put their own copyright notice there when their organization is the author of the source code. However, more often companies fail to include free and open source software copyright notices of 3rd parties and given proper credit to these 3rd parties along with the license information.

Companies embracing open source software need to be aware that such licenses are considered as copyright licenses and not a contractual arrangement only. The effect of this is that when courts consider a copyright infringement in terms of any statutory damages to be paid, the damages are generally higher.

Patent issues sometimes arise when companies embrace open source software. Embracing open source software does not permit a company to just go ahead and infringe a patent belonging to a 3rd party. Embracing open source software is not a 'get out of jail free' card when it comes to 3rd party patents. In one well publicised example, some companies embracing open source software were found to infringe the patents of a major audio and video codec entity. In another example, patented ciphers were found to have been enabled in a piece of open source code.

Care is also needed to avoid the viral effect of open source software licenses. Care is needed that open source software license terms do not turn a company's proprietary software coupled with open source software all into open source software. Open source software licenses can require the contributors and the distributors to give a license to their IP rights for use in the open source software. All such licenses include copyright license. Some licenses include explicit patent license. A company needs to take care in case no explicit patent license is included if there is an implied patent license. The "viral effect" here means that the license given by the distributor is not limited to the open source component used or modified. There is therefore a risk of neutralising a company's control and value points. This issue depends very much on the open source license type in question.

So, in summary:

In this video, we focused on exploring many of the different types of IP related risks a company may face. Subsequent videos in this series will cover the following topics

- IP risk management process
- IP risk mitigation solutions

- IP risk register
- IP risk visualisation
- The psychology of IP risk management

Conclusion

Many thanks there to Donal O'Connell for this fantastic introduction. In our next session, we will join Donal for a deeper dive into the management processes that are needed and how these can be mastered before disaster occurs! Thanks for watching and see you on Module 2.