IP Risk and IP Risk Management

The psychology of IP risk management

Introduction

Hello and welcome to the Academy by PatSnap course on IP Risk. For this series, 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. Donal O'Connell, Managing Director of Chawton Innovation Services, will be our host for this session covering the psychology of IP risk management. So Donal, it's over to you. Thank you.

Ok, let's start with the psychology associated with risk:

Now, there are a variety of psychological factors which influence how people react to risks. Research conducted on this topic has helped to understand people's risk perceptions; how "rules of thumb" influence how people evaluate risk; how risk perceptions influence people's concern about risk; and how optimistic biases influence how people react to risks. Some of the key learnings are as follows:

- People assess the frequency or probability of a risk by the ease with which instances or occurrences of that type of risk come to mind.
- People assess risks starting from some initial starting point, from which they then adjust to a final point as they complete their analysis. This initial starting point is called the 'anchor'. Not everyone has the same anchor or starting point.
- When asked to rate their chances of being adversely impacted by a risk, more people tend to rate their own chances as above average. They believe that negative things are more likely to happen to other people and positive things are more likely to happen to them.
- People interpret risk information in a self-serving manner. People think that signs of a risk materializing happen early, and if they have not seen any signs, then the risk is not going to happen.
- People employ 'ego-defensive' mechanisms to downplay their risks. People who are engaging in risky behaviour or are exposed to risks will downplay their risks and give reasons to justify their behaviours, which are often ineffective precautions.
- People tend to under-estimate the impact if they fall victim to some unfortunate event. So they are inclined to ignore the risk, thinking that even if it does happen, they will be able to cope.
- People believe they have more control over a situation than they really do.

OK, so what has this got to do with intellectual property?

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.

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 about 80% of the total value of many companies. There is no data available on the scale or size of the risks associated with IP facing companies, but one can assume that it is significant, and probably around this 80% mark.

Not all IP 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, etc.), the source or origin of the IP related risk, the impact and probability of the IP risk, the date when the risk is likely to materialize, the geographical nature of the IP risk, whether they are generic or specific in nature, the group or sub-group within the organization most impacted by this risk, and so on and so forth.

I would argue that every organization faces IP related risks.

Ok then, let's take a look now at how companies react to IP related risks…

Based on my own personal experiences over the past dozen or more years working in the IP sector, interviews with a number of knowledgeable IP professionals in recent times as well as some benchmark data gathered from various IP change projects I have conducted, I've found that there are three different approaches being taken by companies when it comes to IP related risks:

- There's: Denial mode
- Reactive mode
- And: Proactive mode

Let's explore each of these, starting with Denial mode:

Denial is the refusal to accept or believe that the organization faces any IP related risks. It may seem strange that companies would embrace such an approach but many do. However if we look back at some of the psychology associated with risk, perhaps this denial mode is then easier to understand.

Perhaps such companies find it difficult to find instances or occurrences of IP related risks that come to mind. Perhaps their 'anchor' or starting point is different from others. Perhaps they believe that negative things associated with IP only happen to others. Perhaps because the IP related risks are not happening now at this moment in time, they can be dismissed. Perhaps they see no early signs of IP related risks.

That said, denial is listed as an immature developmental defence along with delusion, distortion and projection in the Diagnostic and Statistical Manual IV of the American Psychiatric Association. It is therefore not an approach I personally would suggest for addressing IP related risks.

Ok, what about Reactive mode?

In reactive mode, the behaviour of the organization is not internally motivated but manifests in response to a situation or the actions of others. When an IP related risk materializes, then and only then does the organization react. Reactive change occurs when an organization makes changes in its IP practices after some threat has already occurred. Reactive aims to deal with the consequences of an IP risk.

However, operating in reactive mode has some major drawbacks, in that many solutions to help mitigate IP related risks are ‘off the table’ once the IP related risk has materialized. It is very difficult to take out house insurance if your house is already up in flames.
Reactive mode is sometimes referred to as firefighting, the emergency allocation of IP resources, required to deal with an unforeseen IP problem. Just as in the real world, there is an assumption that "fires" are unpredictable and that they must be dealt with immediately.

However, a too-frequent need for emergency IP action may reflect poor planning, or a lack of organization, and is likely to tie up valuable IP resources that are needed elsewhere.
When IP related risk work consists almost entirely of fighting fires, rather than dealing with things in a rational, prioritized manner, and devoting some time to medium-term and long-term issues, then a serious problem can arise. The problem is, that once you are in firefighting mode, the lack of medium and long-term focus just causes more IP fires to pop up down the road. Hence, it is a vicious cycle, and it can eventually wreak havoc on the morale of the overworked IP resources. Also, stress related to continuous firefighting becomes an issue of concern.

To keep firefighting to a minimum, the proactive approach is recommended, which includes the attempts to foresee, and protect against, such IP related emergencies. I fully accept that there are instances in the world of IP when the reactive mode is the only option but it should not become the norm.

So let’s examine Proactive mode:

Proactive behaviour involves acting in advance of a future IP situation, rather than just reacting. It means taking control and making things happen rather than just adjusting to an IP situation or waiting for something to happen.

Organizations that operate in proactive mode are those that treat IP risk management with the same level of professionalism as the other core IP processes. They work to identify IP related risks early; conduct analysis of potential risks; prioritize these IP related risks; and then take the appropriate IP risk mitigation actions if and when needed.

Companies that operate in this proactive mode also tend to have an established network of specialist IP risk solution providers, such as defensive aggregators, IP insurance providers, anti-counterfeit specialists, and so on...

The psychology associated with risks says that powerlessness makes any risk feel scarier. However, operating in proactive mode empowers the organization - as people are typically less concerned about risks that are known, observable, have immediate effects, and/or which can be mitigated against.

Once a company operates in proactive mode for a period, their ability to properly assess the impact and probability of an IP related risk greatly improves; their 'anchor' or starting point when conducting IP risk analysis is more realistic; they rate their chances of success more sensibly; they avoid interpreting risk information in a self-serving manner; they drop any ego-defensive mechanisms; they are more honest when assessing their level of control; and last but not least they just become better at mitigating IP related risks.
IP risk appetite, tolerance and threshold:

Apart from the three different approaches (denial, reactive and proactive) with respect to IP risk management outlined above, there is another aspect to the psychology of IP risk management worth exploring, namely IP risk appetite, tolerance and threshold.

IP risk appetite is defined as the amount and type of IP related risks that a company is willing to take in order to meet their strategic objectives. Companies will have different IP risk appetites depending on their sector, culture and objectives.

While IP risk appetite is about the pursuit of risk, IP risk tolerance is about what a company can actually cope with.

IP risk threshold takes both the uncertainty and the impact into account when determining whether a company takes a specific interest in an IP related risk or not. Below the IP risk threshold, the organization will accept the IP related risk. Above the IP risk threshold, the organization will not tolerate the risk.

Frequently, the terms IP risk appetite, IP risk tolerance and IP risk threshold are used interchangeably, although they represent related, but different concepts.
I favour focusing on the IP risk threshold as it takes both impact and probability into consideration.

It should be stated that the IP risk threshold level for a company cannot really be set to zero as companies have to take some IP related risks but avoid others.

When the IP risk exposure crosses above the IP risk threshold level set, IP Management has to take decisive actions to bring back the IP risk exposure under that level.

What is the right IP risk tolerance level for a company?

There is no right level for the IP risk threshold level for a company as it will change over time. I suggest however that there are three general phases for a company with respect to their IP risk threshold level.

Starting with Phase 1:

When a company first embraces IP risk management, I suggest that a company should set its IP risk threshold level very low to ensure that the vast majority of IP related risks in their IP risk register are at least analysed and reviewed and very few IP related risks are ignored.

Then, Phase 2:

Once the company becomes more mature and sophisticated in terms of IP, IP management and IP risk management, I suggest that the IP risk threshold level can be raised by the company so that attention focuses very much on those high impact and high probability IP related risks.

Finally, Phase 3:

After a period of time, I suggest that the company should slowly but surely lower its IP risk threshold level, so that mid impact and mid probability IP related risks get properly addressed. If the company leaves its level high, it may mistakenly believe that it faces no IP related risks.

So, some final thoughts:

Yes I am huge fan on this proactive mode. Proactive mode is about taking preventative measures, ideally aiming to stop the IP risk before it happens. It is about prioritizing risks, prioritization being a combination of the possibility of the risk occurring and estimating the impact. It is however not just about analyzing the possibility that some risk will actually occur, but also making sure they have a recovery plan in place, and that the recovery plan has been stress tested.

Companies need to operate in proactive mode, carving out time in their schedule for IP risk management, and taking responsibility to ensure that they have a good fit for purpose IP risk management process in place underpinned by a robust IP risk management tool. Companies also need to give some consideration to their IP risk appetite, tolerance and threshold, but focus especially on their IP risk threshold.

Conclusion

Well that ends our series on IP risk. Thanks very much to Donal O'Connell for compiling this valuable information. Please be aware that we have a range of support material on Academy by PatSnap to help further investigate this topic. We hope you enjoyed this series and do reach out to us with your feedback, we'd be glad to hear it. In the meantime, please take a look at our other material and, until next time, good luck and thanks for watching.