FORUM

IP Risk Management

How to mitigate IP risks in a VUCA world

About the author

Donal O'Connell is the Managing Director of Chawton Innovation Services which offers consultancy in the areas of innovation and IP management. He is formerly a VP of R&D and a Director of IP at Nokia where he worked for 21 years and gained wide and varied experience in the wireless telecoms industry. Donal is the author of a book on ‚Intellectual Property Risk Management' which was published in early 2022.

Dear Reader

We are pleased that you are interested in our white paper. In the following, you will receive valuable insights on IP risk management. These insights are intended to give you an idea how to manage this process effectively and efficiently. You can deepen your knowledge of the topic with the training courses we offer on IP risk management.

Best regards,

Alexandre Hô

Jean-Claude ALEXANDRE HO
LL.M., Maître en Droit
Conference Manager Intellectual Property
FORUM • Institut für Management GmbH

IP risk management

What is the connection between IP and risk?

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. However, many ignore the risks associated with IP or only react when the risk has materialized, which is most times too late.

What are some examples of IP related risks? The obvious IP related risk is that a business may infringe the IP rights of a 3rd party. However, there may also be IP related risks associated with for example:

- Having too narrow a definition of IP, and ignoring potentially valuable IP assets
- The IP terms and conditions in some development or commercial agreements with 3rd parties
- The publishing activities of the business
- Embracing open source software
- Being involved in certain interoperability standardisation activities
- Getting involved in some open innovation initiatives
- The use of subcontractors
- One‘s own IP out-licensing program
- Employees stealing IP from the company
- The scourge of Counterfeit products
- Trademark disputes with 3rd parties
- Trade secrets not being properly managed

Are IP related risks a significant issue?

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 of the risks associated with IP but one can assume that it is significant, and probably around this 80% 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 products, patent litigation, trademark disputes, data hacking and so forth.

The bottom line is that IP related risks are a significant issue for many companies.

Are all IP related risks generally the same or not?

All IP risks are not the same, far from it. 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 (e.g. patents, trademarks, copyright, 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 materialise, the geographical nature of the IP risk, whether they are generic or specific in nature, the group or subgroup most impacted by this risk in the organisation, etc.

Where do IP risks originate?

Many mistakenly assume that all IP risks originate from competitors, but IP related risks may originate from a variety of sources:

- The activities of one’s own company and its people
- The activities of entities within one’s own eco-system (suppliers, partners, distributors, customers)
- The activities of one’s competitors
- The activities of other entities such as NPEs

- Changes to Government policies related to IP
- The activities of illegitimate entities such as hackers and counterfeiters

What is IP risk management?

IP risk management is a practice that deals with processes, methods, and tools for managing IP risks in a project, business unit or organization. It is initially about the identification, assessment, and prioritization of IP related risks followed by the coordinated and cost-effective application of resources to reduce or eliminate the probability and/or the impact of these IP related risks to the organization.

IP risk management involves understanding, analysing and addressing IP related risks to make sure organizations achieve their objectives. So it must be proportionate to the complexity and type of organization involved. Proper IP risk management is an integrated and joined up approach to managing IP related risks across an organization and its extended networks.

IP risk management is about ensuring that the business really understands its IP related risks, and then mitigates pro-actively. The rationale for this may be driven by the need for freedom to use technologies already in use or being considered for use in the company's products, but there are many other reasons why businesses need to take IP risk mitigation seriously.

The focus should be on risk mitigation and not just of risk evaluation. Risk mitigation covers efforts taken to reduce either the probability or consequences of a threat. Risk mitigation efforts may range from physical measures to financial measures.

What are the key steps in the IP risk management process?

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.

At a very top level, the IP risk management process involves the following key phases:

- Identification
- Analysis
- Review
- Mitigation
- Monitoring

Which approach, top down or bottom up, is best for IP risk assessment?

The two 'halves' of IP risk management are IP risk assessment and IP risk mitigation. Risk assessment is about the identification, quantification and prioritization of IP related risks facing an organization.

In the top-down approach, IP risk management begins at the highest conceptual level and works down to the details, with the major IP related risks being identified by senior management.

In the bottom up approach, it begins down with the details and works up to the highest conceptual level, with IP related risks being identified by middle managers and individual contributors, and with the higher probability and/or impact IP related risks then being passed up to senior management.

Top down and bottom up are both strategies of information processing and knowledge ordering, used in a diverse range of fields, including in the area of IP risk management. The two approaches may be seen as a style of thinking. Processing here is just a simpler way to say taking in IP related

risk information, analysing it, and drawing conclusions or taking action. In a top down approach, an overview is formulated, with the details beyond that overview specified but not delved into.
A bottom up approach is the piercing together of different details. It should be stressed that both have the same goal, namely to ferret out the key IP related risks facing the organization.

Success depends on using a combination of top down and bottom up approaches to first identify, classify and prioritize the IP risks facing the organization.

Combining top-down with bottom-up approach is especially needed when the IP environment is continuously changing and consequently, the organization's IP risk map is shifting. In such circumstances, the top-down approach gives IP risk management the necessary strong foundations whereas the bottom-up approach give it some flexibility.
The combined approach also keeps everybody in the organization involved in the IP risk management process and ensures accountability and improves compliance.

For organizations tackling IP related risk management for the first time, it is recommended to start initially with a top down approach but then to roll out a bottom up approach to reach out across the entire organization over time. The bottom up approach may for example become an annual exercise conducted across the organization.

How does one mitigate IP related risks?

There are a variety of IP risk mitigation techniques available, but of course their effectiveness will vary from one particular IP risk to another, on timing, and from business to another.
Some of the IP risk mitigation techniques are listed here, but this list if not exhaustive by any means:

- Raising awareness of the importance of IP across the organisation
- Leveraging technical cooperation with others
- Using Standards with fit for purpose IP policies
- Obtaining indemnities
- Participating in patent pools
- Licensing IP
- Designing around
- Finding prior art to invalidate 3rd party IP
- IP acquisition
- Taking out IP insurance

It is important that a company builds up a good understanding and appreciation of the various IP risk mitigation solutions which exist, and if and when they should be deployed. There are a growing number of specialist external IP risk mitigation solution providers which should also be considered.

What are the components of a good IP risk management solution?

IP risk management is not easy and a number of components need to be in place for a company to truly master this aspect of IP. I strongly suggest that the following components are needed:

- Good IP and IP related Risk awareness and education
- A robust fit for purpose IP Risk Management process
- IP Risk Management system / tool
- Data (IP related risks, actions, documents, reports)
- A variety of IP Risk Mitigation solutions
- IP Risk Management resourcing (people, budget)
- Proper IP Risk Management governance

Who should be interested in IP risk management?

Anyone interests in IP should take IP risk management seriously. It should be of particular interest to anyone:

- Operating in an IP litigious environment
- Coming up for exit or listing
- Anxious to get IP risk management under control
- Whose executive management team are

demanding visibility of IP related risks

- Experiencing major business changes
- Facing a major IP risk and realising that they are unprepared
- Interested in proper governance of IP

Regardless of why one is interested, it is best to master IP risk management when things are calm rather than when one is tackling a major IP risk, when pressure is intense and everything seems chaotic and dis-organized. This is not the right time for a GC, CIPO or IP Manager to have to go to the Board and explain that the IP risk management process is to 'panic widely and run away'.

What are the keys to success in IP risk management?

I suggest that IP awareness and IP governance are like the bookends, keeping everything else in proper order. Governance here is about management putting IP risk on their agenda and regularly asking themselves whether they have the right culture, people and processes in place.

The skills needed to succeed with IP risk management do not match exactly those needed to be successful with the other key IP processes, such as IP creation, IP portfolio management, IP exploitation and IP enforcement. The mind-set is just different for those charged with IP risk management.

Any final thoughts?

It is important not to underestimate or exaggerate the risks associated with IP. As IP relates to innovation and creativity, it can sometimes be an emotive subject and some care is needed.

Trade secret management

Trade Secrets

Trade secrets constitute an important part of a company's intellectual property portfolio and they are generally any practice or process not known outside of the company. Specifically, for a practice or process of a company to be considered a trade secret it must fulfil three criteria:

- it must be secret (i.e. not public information),
- it must provide an actual or potential economic advantage for the company,
- it must be actively protected (i.e. the company exercises reasonable measures to maintain it as a secret).

Some examples of trade-secret include scientific processes, formulas, product blueprints, algorithms, raw or processed data, software, manufacturing processes, customer lists, financial information, market research studies, internal costing and pricing information, etc.

The neglected step-child of IP

Although trade secrets have been the neglected step-child of IP, this is slowly but surely changing for a variety of reasons:

- Law changes (DTSA in USA; EU Directive on Trade Secret in Europe; Anti Unfair Competition Law in China, etc.)
- Increased trade secret litigation particularly involving US companies but not exclusively so
- Growing interest in trade secrets by the tax authorities (e.g. OECD BEPS Guidelines, Patent Box Tax Regimes including trade secrets as qualifying IP)
- Cyber criminals trying to steal trade secrets
- Companies embracing Open Innovation and sharing trade secrets with one another
- The changing nature of employment
- Pending trade wars which some link to trade secret theft
- IP reform weakening some other forms of IP

Trade secrets are a very important part of any IP portfolio. It is no exaggeration to say that virtually every business possesses trade secrets, regardless of whether the business is small, medium or large. Trade secrets are an important, but oftentimes an invisible component of a company's IP portfolio of assets. However, trade secrets can also be the crown jewels within the portfolio.

The top level process for managing trade secrets

Processes are not just reserved for registered forms of IP like patents and trademarks. I would arguethat process thinking is even more critical when it comes to unregistered forms of IP like trade secrets, as there is no external entity like the Patent & Trademark Office holding the hand of the organisation and keeping it on the straight and narrow.

I suggest that the trade secret asset management process at the very top level consists of the following key blocks or steps – context; identification; analysis; review; protection; and monitoring.

The key steps in that process

Context: Understanding the environment in which you are operating from an secrecy perspective.

Identification: Working to identify information within the organisation which may warrant being treated as a trade secret, since the definition of a trade secret is very broad indeed.

Analysis: Evaluating the information, classifying it, determining who has access and who needs access going forward, etc.

Review: Deciding whether to go ahead and treat this information as a trade secret or not as the case may be. This as such is a business decision.
Protection: Putting the appropriate administrative, legal and technical protection mechanisms in place to ensure that the information has ‚reasonable' protection in place going forward.

Monitoring: Sanity checking on a regular basis go-

ing forward that the information still warrants being treated as a trade secrets, that it is indeed being protected and if any other factors have changed as far as this trade secret is concerned.

Some other processes

There are some other processes to consider when dealing with trade secrets.

These include the sharing of trade secrets with others; the protection of trade secrets when a new employee joins the organisation as well as when an existing employees leaves the organisation; the handling of trade secrets when major corporate events take place (e.g. some M&A activity, an investment round); the logging and tracking of the costs associated with trade secrets; the valuation of the trade secrets across the organisation; the management of the accidental or deliberate disclosure of a trade secret; and the handling of trade secret disputes and court cases.

The foundations

The strength of any process however lies in its foundations.

The trade secret asset management process requires some good foundations, including ...

- trade secret education of employees to help raise awareness, understanding and appreciation of this rather unique form of intellectual property
- a fit for purpose trade secret policy, i.e. a deliberate system of principles to guide decisions and achieve rational outcomes with respect to these valuable assets in the organisation.
- a robust trade secret system or tool that underpins the process, and thus help to improve efficiency and effectiveness
- good quality trade secret metadata (as without data, an organisation has no information, and without information, an organisation has no knowledge)
- trade secret asset management governance, i.e. the way rules, norms and actions are structured, sustained, regulated and held accountable in the organisation

Final thoughts

In response to competitive pressures and ever-changing conditions, many IP function are fundamentally rethinking the way they do business. It is most important to be able to clearly link your IP function's processes and organisational services to your business goals and objectives.

As IP functions strive to keep up with ever-changing customer demands and market needs, there is a growing demand for modelling and analysis of the IP function's core processes, in order to capture the strategic relationships within the IP function itself and with external partners and players as well, so as to identify areas for improvement.

Given the growing importance of trade secrets, it is imperative that IP functions give some serious thought to their process for managing such assets.

You may also be interested in:

Practical Intellectual Property-Management knowledge

Learn the most effective approach to managing portfolios and developing IP strategies in our seminars and courses.
More details.

e-Learning – Click and learn!

The FORUM Institut provides a flexible form of high-quality training: e-learning courses. Choose when and where to learn.
Test now.

FORUM • Institut für Management GmbH • Vangerowstraße 18 • 69115 Heidelberg • Germany
Phone: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.com