

## ***Do You Recognise Intellectual Property as a Corporate Risk?***

If you search Google for the term “Intellectual Property”, you are likely to find references to IP Australia, and government agencies such as the Attorney General’s Department. If you search for “Intellectual Property Policies and Employment”, links to universities abound but commercial companies and other corporate entities are conspicuous by their absence. This paper seeks to put intellectual property on the corporate risk policy agenda.

What is Intellectual Property (IP) and why is it important to consider it as a risk? Intellectual property represents the property of one’s mind or intellect, which includes that of your employee/s. It should be regarded as an asset and treated as you would land, buildings and other valuable property. IP can be an invention, trade mark, original design, logo, marketing campaign or the practical application of a good idea. In business terms, this means your proprietary knowledge - a key component of success in business today. It is often the edge which sets successful companies apart and as world markets become increasingly competitive, protecting your intellectual property becomes essential. (<http://www.ipaustralia.gov.au/ip/index.shtml> 30 Nov 07)

Typically in Australia IP assets are protected in the following ways:

- The application for patents to protect new or improved products or processes;
- Trade marks for letters, words, phrases, sounds, smells, shapes, logos, pictures, aspects of packaging or a combination of these, to distinguish the goods and services of one trader from those of another;
- Designs for the shape or appearance of manufactured goods;
- The automatic application in Australia of copyright for original material in literary, artistic, dramatic or musical works, films, broadcasts, multimedia and computer programs;
- Circuit layout rights (also automatic) for the three-dimensional configuration of electronic circuits in integrated circuit products or layout designs;
- Plant breeder’s rights for new plant varieties; and
- Confidentiality/trade secrets to cover know-how and other confidential or proprietary information.

So who is affected by IP risk and how should you capitalise on, and safeguard your own IP? The fact that you have created IP may not mean that you will own it. You may also need to register your IP to obtain the legal rights of ownership; registration of IP rights in Australia does not always give you international protection. Employees and employers therefore need to take appropriate steps to:

- Understand the value of the IP you own;
- Develop strategies to protect the valuable IP belonging to the organisation;
- Clarify the ownership of IP being used;
- Respect other’s ownership by preventing the inadvertent infringement of a third party’s IP;
- Identify and address IP crimes and infringements in the workplace to ensure increased productivity and to avoid liability;
- Keep a record of original materials brought to the project and materials developed during the project; and lastly, most most importantly
- Develop an IP compliance policy and raise awareness in the organisation.

Different IP rights vary in the protection they provide, often more than one type may be necessary to fully protect your creation. The consequences of not taking the steps outlined above mean that you have few or mainly ineffective controls over a risk that could manifest itself with legal and sometimes criminal consequences.

So what are some possible strategies, actions and policy decisions that need to be taken that will achieve proactive control of IP risks?

Firstly there should be a very comprehensive IP policy clearly articulated to staff, Board members and other important personnel. Secondly, this policy should be part of an ongoing intellectual property education program with the following objectives:

- to alert staff and contractors of their rights, responsibilities and opportunities in relation to intellectual property;
- to alert personnel to any changes to policy, and
- to generate a better understanding of intellectual property issues in general.

At the pointy end of IP protection, if you are seeking patents, do not discuss your design or make it public too soon, as you may lose the legal right to exclusive use of your IP. Make sure that, when disclosing or marketing your invention or design in Australia, you do not invalidate a future patent or design in another country. Ensure you have a method of reporting of inventions and ideas; best practice ensures a written policy stating that all employees must formally document and report inventions and ideas to management.

Such policy statements should be widely available to all employees (use corporate websites) and reviewed frequently. Encourage employees to maintain a logbook to record anything from laboratory notes to sketches, ideas, designs, literature, music or even minutes of meetings, in fact anything where a chronological record of original ideas is useful – regardless of the field or discipline. All company publications and public disclosures should be reviewed to avoid premature disclosure of confidential information.

Many entities have contracts with their employees and contractors. These often describe working conditions and pay, but few mention IP ownership. The reality of today is an ever-changing workplace, where the so-called “new knowledge economy” is demanding that workers have ‘portfolio’ careers and become ever more highly skilled, creative and flexible. Yet who owns their achievements?

Before a contract commences, ownership of IP should be clear and traceable by documenting:

- The IP that is the subject of the contract;
- The ownership and confidentiality of any pre-existing IP or knowledge of the contractor;
- The ownership of the IP developed during the contract;
- The date/s of the duration of the contract;
- The extent, if any, of shared ownership of the IP;
- The extent to which the joint owners may use and commercially exploit the IP once the contract has expired, and
- The nature and proposed use of the IP developed.

Government employees need to be reminded that their work created during their course of employment belongs to the Crown, unless varied by contract. In fact the same is true for all employees; an employer owns the IP produced by employees during the course of employment unless varied by contract.

Many entities fail to conduct exit interviews; this is an excellent time to reinforce post-employment confidentiality obligations. All agreements with contractors, suppliers, manufacturers and distributors should be regularly reviewed to ensure that confidential information is protected.

Employers often recognise that benefits can accrue to staff and the organisation where employees are permitted to undertake work for outside bodies. However, employees should not use any confidential information belonging to their organisation eg an employer’s databases, nor engage in activities that could lead to a conflict of interest such as those in competition with their organisation's

endeavours. It is desirable that there are avenues available for any employee who becomes aware of the unauthorised use of an organisation's IP to report this misuse without fear or retribution. Businesses need to be wary of breaking IP laws on their publications and in the course of their operations generally. Websites can create an area of exposure to breaching IP laws. Logos, images, photographs, artwork, written content and even the design of websites are all copyright material that a company must either own or use under licence. Businesses might "authorising infringement" just by linking to other websites that breach copyright.

(<http://www.news.com.au/couriermail/story/0,23739,22818331-8362,00.html> 30 Nov 07)

Additionally, there is an onus on businesses to ensure their websites do not contain any defamatory material, even when posted by outside visitors. Be especially aware if your site enables users to comment or contribute material that is defamatory, as you may be liable for republishing it, even if you don't know of or review the content.

All organisations have a legal obligation to clear any third party content (works) before they are placed on any of their websites or used within any other documentation. Third party works are those that have not been created by the organisation and cover other people's (including students on work experience):

- Artwork;
- Logos;
- Images;
- Photographs;
- Text;
- Conference papers;
- Published articles; and
- Music etc.

If a third party's work is placed on a website, on a CD ROM or within any other form of documentation without permission, it is an infringement of the third party's copyright, and any copies made of the infringing material will also be illegal copies. Furthermore if the third party's material is changed in any way e.g. shortened, paraphrased, without permission this may be seen as an infringement of the third party's moral rights and legal action may be taken. Before any third party copyright can be placed on a website or in a newsletter or broad publication managers should confirm that:

- Either the content is original content, or
- Ensure that appropriate permissions have been gained in writing from the copyright holder.

It is suggested that there is a central approval point before information is placed on a website; permissions should be kept on an administrative file. To satisfy Moral Rights legislation, the creator should be acknowledged where their material is used.

Indigenous cultural and intellectual property refers to Indigenous peoples' right to their heritage. The heritage of Indigenous peoples' is comprised of all objects, sites and knowledge the nature or use of which has been transmitted from generation to generation, and which is regarded as pertaining to a particular people or territory. Where the creation of an organisation's IP involves the traditional interests or property of Indigenous peoples' and/or the use of traditional knowledge, the organisation should take all reasonable steps to consult with the relevant Indigenous groups to ensure that any decisions taken on the protection, development and commercialisation of that intellectual property conform with the relevant Indigenous protocols and ethical guidelines. For Indigenous communities there are customary laws about disclosure and dissemination of deceased images. Publishers and organisations making content available should also adopt warning and clearances practices.

Attention should also be given to "cyber squatters" when registering company's domain names. "Cyber squatters" are external companies or individuals who might establish an alternative address which is close to the original but with a different suffix, often for "unscrupulous purposes". Cyber squatting cases often involve disgruntled employees or clients who register a .net, .net.au or .biz alternative domain. It is strongly suggested that companies establishing a website address, register as many possibilities as possible in the first instance to protect this form of IP.

One of the greatest risks to any organisation is corporate piracy. Corporate piracy refers to the illegal use of software often through the installation of more copies of software onto computers than licence allows, or the use of counterfeit software. At the Biennial Copyright Law and Practice Symposium held in November 2007 it was alleged that 29% of all business software used in Australia is illegal at a cost of A\$515 million. Across south-east Asia it is estimated (source?) that the counterfeit bill is close to \$7.5 billion.

It is important to note that there is a criminal liability for authorising [aid & abet] IP theft crimes that may be occurring at your workplace. The management of this risk is not difficult or complex but needs a consistent approach to IP awareness, and a no tolerance policy to copyright theft. Once again, appropriate education and training should be introduced so staff understand what intellectual property is, how it affects them, and the significance of IP rights and laws; clear policies and guidelines on the legal use of IP in the workplace; and, appropriate sanctions for breaches of IP rights at work. In addition, regular audits of computer software vs. licences obtained for the workplace help managers of IT systems to identify and remove infringing material, sanction those responsible and ensure that the correct numbers of site licences are purchased to suit the needs of the organisation.

Existing licences with third-party software vendors should be checked to ensure that they authorise the company's intended commercial and geographic uses of the third-party software. All licences should be kept on file in a central place. Work place computers should not be used for illegal downloads of music or films from illegal Internet sites. These steps will have a positive impact not only on your business, but on the whole community as film piracy in the digital age has become more profitable than drug dealing, and is, also known to involve and attract organized crime syndicates.

As previously mentioned, IP is often the most valuable asset of many organisations, however organisations (particularly small ones) often do not dedicate the resources necessary to capture and protect IP. IP audits give business managers an opportunity to analyse their intangible business assets so that the profitability of those assets can be maximized. Effective IP audits should provide managers with a broad analysis of their IP portfolio that evaluates IP according to:

- Strengths
- Weaknesses
- Opportunities and
- Threats

To carry out an IP audit, look closely at your organisation to:

- Identify where intellectual property is used;
- Find out who owns the intellectual property rights; and
- Assess the value of the intellectual property

As the websites <http://www.infoage.idg.com.au> and <http://www.iptoolbox.gov.au> suggest, the strength of an IP Audit lies in the recognition of its existence. Such IP can:

- set your organisation apart from competitors;
- be sold or licensed, forming an important revenue stream;
- offer customers something new and different; and

- form an essential part of your marketing or branding

IP audits help organisations review their products and research work to identify latent IP that has not previously been recognised as valuable. Once IP is identified, steps can then be taken to protect and extract profits from that IP by:

- Protecting it against infringement by others and ultimately defend in the courts your sole right to use, make, sell or import it;
- Stop others using, making, selling or importing it without your permission;
- Earn royalties by licensing it;
- Exploit it through strategic alliances; and
- Make money by selling it

Weaknesses in an IP portfolio often involve ownership issues as outlined above in corporate piracy e.g.

- Lack of ownership entirely;
- Joint ownership with another organisation; or
- Ineffective licence rights.

Some government or other funding agreements include restrictions on IP; check to see that appropriate IP indemnification and disclaimer language are included in all company contracts; such weaknesses can be discovered and mitigated through an IP audit.

Opportunities revealed in IP audits include helping an organisation to receive financing. Venture capitalists, other investors, and state and federal government grant administrators often require assurances that a business owns its IP and that threats against that IP are recognised and managed. IP showing as an asset in the balance sheet may be positive news for shareholders.

An audit of a competitor's IP may determine whether the competitor's products and services might infringe your own organisation's patents, copyrights or trademarks

IP audits can help reveal both indirect and direct IP threats to an organisation. Indirect threats may result from:

- Unpaid patent maintenance fees that may result in a business's patents lapsing prematurely and unintentionally;
- Loss of potential domain name or trademarks through not being registered; and
- Loss of unsecured business and marketing plans, pricing and financial data, customer lists, product formula, research and development

Whilst direct threats would include IP infringement suits, where third parties sue for infringement of their patents, copyrights, or trademarks

So, is there a preferred approach to IP risk control? There should be a mix of controls. Some as outlined above are strategic e.g. IP Policy and education of personnel, employment contracts outlining IP ownership and protection. Some are operational e.g. IP Registers, IP Audits; other risks may be transferred e.g. requesting permission to use third party IP. It is important that your IP Policy contemplates and is designed to meet the specific exposures and needs that your business has.

Whatever the approach, effective risk policy and risk management should be applied to preserve a company's IP and protect it from unintended or even fraudulent use of other's IP.