More than reputations at risk

Brands, patents and trademarks are among a new class of so-called intangible assets that are rising up the risk agenda. They are easily broken, but can you insure them? By Garry Booth

Risk managers and insurers found it hard in the past to get their heads around intangible risks. But today's risk professionals are increasingly aware that when an intangible risk materialises, it becomes very tangible indeed.

Recently, for example, users of the ubiquitous BlackBerry were almost left without service because its maker, RIM, was sued by a patent-holding business that claimed RIM had stolen its technology. RIM settled for $612.5 million and 'CrackBerryheads' around the world breathed a sigh of relief.

Intangible risks

Such a threat against a business's intellectual property (IP) is a classic example of intangible risk. But intangible risks are everywhere and growing. Patents, copyrights and licenses, brands, trademarks and images are all now valuable assets in the modern business world.

It was not always so. Company valuations used to be easier because they were largely determined by capital assets you could touch, such as plant and equipment. According to PricewaterhouseCoopers, intangible assets now probably account for more than half of the market value of the average listed company worldwide.

It follows, then, that if a company's intangible asset portfolio is growing, so is its intangible risk portfolio. Peter Hacker, Head of the Communications and Technology Industry Practice at Jardine Lloyd Thompson, says that the market capitalisation of technology, media and telecom companies in particular correlates strongly to the patent portfolio that they are holding.

Patent infringement is moving up the corporate risk agenda fast. "It's because there is a lot of uncertainty around patent laws," explains Hacker. "The EC has different patent laws to the US. That's leading to patent trawlers trying to find ways to sue against potential infringers under different law systems and different jurisdictions."

The cost of exposure

Privacy issues are driving awareness of intangible risk in different industry sectors, says Phil Mayes, Senior Underwriter at Zurich Global Corporate. "Recent incidents of major enterprises losing data show that data leakage is a real problem," says Mayes. "The sectors most at risk are retail, financial institutions and healthcare." Exposures are increasing as more companies' networks are internet-protocol based, he adds.

INTANGIBLE RISKS FROM ALL DIRECTIONS

There are four main groups of intangible risks from a third-party liability perspective:

1. **Intellectual property risk,** including copyright, patent and trademark rights infringements.
2. **E-commerce transaction risk,** including data encryption.
3. **Operational risk,** such as negligent breach of contractual and non-contractual duties – including privacy.
4. **Data protection and infringement.**

Intangible risks from a first-party point of view include issues related to computer malfunction, breach of IT security and online/offline fraud.

Dawn Simmons, Partner in Jardine Lloyd Thompson's Cyber and IT Risks Team, agrees and points out that companies that do not take precautions are exposing themselves to serious regulatory risk. "There has been a wealth of regulation, especially in the US, covering best practice, compliance, and fines and penalties, aimed at companies that do not protect the sensitive personal information that they hold," she says.

The UK Financial Services Authority last year fined Nationwide Building Society £980,000 for failing to take reasonable care to ensure it had effective systems and controls to manage risks relating to information security.

Michael Brown, Senior Insurance Consultant with the law firm Allen & Overy, has extensive experience of advising commercial insurance buyers and lenders on insurance and reinsurance policies. He defines an intangible asset as something an accountant can attribute a value to but that cannot be touched: "That could be goodwill, it could be IP rights, it could even be landing slots at Heathrow," he explains.

Brand and reputation are increasingly at risk. "Goodwill based on branding has always been a key asset in business," says Brown. "But these days it is easier to lose it. Today when something happens the whole world knows about it in a matter of hours. There is more competition in commerce, intangible values are higher and there is more litigation."

Intangible risk management

But risk managers are becoming more switched on. Dan Trueman, an underwriter specialising in intangible risks at the Lloyd's insurer Kiln, says that risk managers are becoming more sophisticated in their outlook on intangibles.

"Risk managers increasingly relate to the C-suite executives. Once, risk management was more to do with fire prevention and safety, protecting physical assets," he says. "Nowadays, with the onset of enterprise risk management and continuity planning, risk management has become a more financial role and the risk manager is more aligned with the CFO." Both increasingly realise that the important insurable interest is not necessarily a physical asset but it is the revenue stream from an intangible asset, Trueman believes.

But does that mean risk managers will soon be able to buy insurance for all their intangible risks? Insuring intangible assets, such as reputation, is much more difficult than insuring physical assets because it is hard to put a price on the risk. "Even with business interruption, which is notoriously hard to price, potential losses can be »»

"The potential exposure of a Fortune 500 company to an intangible risk such as intellectual property is in the billions and that's why most underwriters are terrified of it."

Peter Hacker, Jardine Lloyd Thompson

»» quantified. That's often not the case with intangible assets," says Brown.

Innovative solutions

But the insurance industry is moving in the right direction. "The potential exposure of a Fortune 500 company to an intangible risk such as intellectual property is in the billions and that's why most underwriters are terrified of it," Hacker says. "But we can tap up to $150 million limit which could be valuable to a lot of companies."

Hacker's team is also working with insurers to extend the scope of intangible risk transfer. A groundbreaking non-damage business interruption product is now available. It protects a business's gross margin loss plus the increased costs of working caused by intangible events such as supplier failure, product recall, cyber attack or the loss of a key patent.

Insurers and risk managers will have to adapt to an evolving and complex risk landscape, however. Mayes at Zurich sees more risks gathering on the horizon and believes network security will be more important to businesses. "I foresee cyber extortion and distributed denial of service attacks becoming more prevalent as sophisticated criminals target networks," he predicts. "The key targets will be those companies that rely on bandwidth – online trading companies, for example."

Looking further into the future, Mayes says that the trend towards a wireless world could heighten vulnerabilities. "Everything that was 'e' is becoming mobile and the increasing availability of mobile broadband will exacerbate this issue," he warns.

Trueman believes that defining reputational risk will become more important: "How do stakeholders put a value on a company's reputation and what can they do to protect it? That will be an increasingly important question." He says that tackling intangibles like reputational risk will take more collaboration between insurers, brokers and their clients, "so that companies know what they are buying and we know what we are selling, to achieve genuine risk transfer. Collaboration will create better value products." RS

i Peter_Hacker@jltgroup.com

Garry Booth has been writing on emerging risks and risk transfer for the last 25 years. He is co-editor of the monthly journal *Future Risk*.

CYBERCRIME WAVE BECOMES A TSUNAMI

Threats from cyberspace are everywhere and growing, according to experts. More and more businesses are falling victim to cybercriminals. The problem has reached such a level that many businesses no longer have any confidence in the authorities to do anything about it.

A survey of the 3,500 members of the Corporate IT Forum found that 69 per cent reported seeing increases in the amount of hi-tech crime committed against them. Firms are being hit by viruses, denial of service attacks and website defacements, the survey said. The variety and intensity of attacks has led many to believe that hi-tech crime has been taken over by professional criminals.

In another survey, online identity firm Garlik says there has been a sharp rise in online financial fraud, with more than 250,000 incidents reported in 2007 – a 20 per cent rise on the previous year. The report highlighted a growing professionalism among online criminals, with personal and credit details being traded online. Garlik says that the information black market had doubled, with more than 19,000 illicit traders identified.

Cybercriminals are not only interested in financial gain. There has also been a steep increase in what is known as 'hacktivism'. Governments are now so concerned about the activities of so-called cybermilitias of politically motivated hackers that NATO founded a cyberdefence centre in Estonia earlier this year. The move was prompted after the country was hit by a wave of 'distributed denial of service' attacks following a row with Russia.