

# **The Real World Business of Intellectual Property Protection\***

by

**Raj Aggarwal**

**Dean and Frank C. Sullivan Professor of International Business and Finance**

**College of Business Administration**

**The University of Akron, Akron, OH 44325**

**330-972-7442; [aggarwa@uakron.edu](mailto:aggarwa@uakron.edu)**

**March 2009**

**Keywords: Intellectual Property, Technology Strategy, R&D, Counterfeiting,**

**\* This paper is based in large part on a November 13, 2008 panel discussion sponsored by the University of Akron College of Business Administration and the Northeast Ohio International Business Network. This panel was moderated by *Dr. Raj Aggarwal*, Dean and Sullivan Professor of International Business & Finance at The University of Akron's College of Business Administration and included panel members *Diane Dominick*, Director, Business Development, STERIS Corporation, *Jackquelyn Strickland*, Senior Counsel, Intellectual Property, The Diebold Company, *Steve Petras*, Partner, International Practice Team Leader, Baker & Hostetler LLP, and *Don Esarove*, President, Cypress Corporation. While the author thanks panel participants for their thoughts and contributions, the attendees and other colleagues for useful comments, and Joe Rich for research assistance, the author remains solely responsible for the contents and any remaining errors.**

# **The Real World Business of Intellectual Property Protection\***

## **Abstract**

**Intellectual property protection and management (IPPM) are important operational and strategic issues especially for global companies. Most prior discussions of this topic focus heavily on the legal aspects of this topic. However, this paper argues that the non-legal aspects of IPPM are just as, if not more, important in practice. It provides some guidelines and practical advice for companies that would like to improve their IPPM processes.**

## **Introduction:**

**Given the ease with which information moves across borders, companies competing internationally need to develop and implement proactive policies to adequately protect and manage their intellectual property. This is especially important as IP, and not physical assets, is increasingly the major source of wealth creation.<sup>1</sup> Further, it is widely recognized that IP may be a critical differentiator between companies in terms of sustainable competitive advantage.<sup>2</sup> Finally, these days IP is being developed all over the world regardless of the headquarters location of a company.<sup>3</sup> In spite of its importance IP protection and management policies seem not to receive appropriate senior management attention.<sup>4</sup>**

**Management policy needs to go much further than the mere legal processes of protecting patents, trademarks and copyrights, as well as all other sorts of confidential information especially as remedies can be slow, ineffective, and costly. Operating policies and practices should be the first defense and can help minimize costs of IP protection and can help realize the greatest value from your intellectual property portfolio.**

## **Why is Your IP at Risk?**

**Why will others try to infringe on your IP? They think you are making money off the idea and they too want a share of that, according to Mr. Steve**

---

<sup>1</sup> See, for example, Raj Aggarwal, "Globalization of the World Economy: Implications for the Business School" *American Journal of Business* 23 (No. 2, Fall 2008): 5-12.

<sup>2</sup> See for example, Teece, David J., "Explicating Dynamic Capabilities: The Nature and Microfoundations of Sustainable Enterprise Performance" *Strategic Management Journal* 28 (August 2007): 1319-1350.

<sup>3</sup> See for example, Hayashi, Takabumi and Manuel G. Serapio "Cross Border Linkages in R&D: Evidence from 22 US, Asian, and European MNCs" *Asian Business and Management* 5 (2006), 271-298.

<sup>4</sup> Even when CEOs appreciate the importance of intellectual property, many see it as a safe thing to delegate, with researchers, designers and engineers creating it; lawyers filing patents; and marketers selling it. "The problem with IP is that it's technical in its essence," says Steve Davis, CEO of Corbis, the image licensing firm founded and owned by Bill Gates. "It's very simple to wave and say, 'Somebody else has to deal with that.'" *Chief Executive*, November 2004.

**Petras, Partner, International Practice Team Leader, Baker & Hostetler LLP in Cleveland, Ohio. Companies need to be aware of counterfeiting threats to products and practices in foreign markets originating in countries with weak IP laws and enforcement, such as China, and need to create a plan to actively prevent any infringements. It is important to publicize the counterfeit products since most people, even in foreign markets, do not want to buy a copied good, they want the real thing. There is an Anti-Counterfeiting Coalition made up of businesses that publicize the counterfeits. Procter & Gamble at one time felt that they owned the whole market in China, but over time knock-offs increased market share and P&G lost market share. By exposing the frauds and counterfeit products, they were able to begin to reclaim market share. It is also important to train employees so they recognize when counterfeiting occurs. The sooner these counterfeits are recognized, the sooner you can take actions to stop them. Sometimes it may be necessary to hire a private investigator, especially in markets where you do not have a physical presence. Finally, Mr. Petras notes that you should advise your CEO that legal enforcement against counterfeiters can be quite expensive so it is best to start with non-legal remedies.**

**Sometimes your IP may be at risk, not from a hacker or counterfeit threat, but because your patents are not very strong and are easy to get around. This requires a creative protection approach. For example, GE obtained a patent for their self-cleaning oven, but it was easy to get around since it was just a series of locking mechanisms. Instead of trying to enforce their IP rights or license the technology, GE gave it away to other oven manufactures if they paid GE \$5 for every oven sold with the technology – this is a win-win situation for all parties involved. Another example is Microsoft, which is faced with anti-trust action in the European Union. Microsoft may have to license or lease certain programs so others can make their software products using Microsoft's platforms.**

### **Evidence on International Threats to IPPM**

**Consider this scary thought that Richard Clark, former member of the U.S. National Security Council under both Presidents George H.W. Bush and William Jefferson Clinton, shared with Dr. Raj Aggarwal, Dean of the College of Business Administration at the University of Akron: China has hacked into many corporate networks and has obtained corporate secrets that are of interest.<sup>5</sup> It's not just corporate America that is at risk. The Pentagon has encountered a cyber attack so severe that "it has taken the unprecedented step of banning the use of external hardware devices, such as flash drives and**

---

<sup>5</sup> Discussion at a Cleveland Council of World Affairs lunch for Mr. Richard Clark in October 2008.

DVD's".<sup>6</sup> Even NASA has had secret information stolen, with the suspects having links to the Chinese and Russian governments.<sup>7</sup> *Business Week* reported that "a still undetermined amount of information about the Shuttle [was sent] to a computer system in Taiwan" (the Chinese government will often use Taiwan as a "digital weigh station"). By December 2005 "at least 20 gigabytes of compressed data-the equivalent of 30 million pages – were routed from NASA's Johnson center to the system in Taiwan".

This breach was not the first at NASA. As early as 1998, a US-German satellite became useless when it abruptly turned toward the sun. The cyber code for this event may have come from Moscow. In 2002, rocket engine designs may have made their way to China. As recent as 2007, a breach occurred at the Goddard Space Flight Center. John W. McManus, former NASA chief technology officer, pointed out that "If another country can break in and steal information about rocket motors or fuel systems, well, that's billions of dollars that can be spent elsewhere". This is particularly scary because "seizing space dominance is the root for winning war in the Information Age," Li Daguang, a researcher at the government-backed Chinese Academy of Sciences, wrote in a 2004 publication of the People's Liberation Army, *Zhongguo Guofang Bao*.

Of course, China and Russia deny employing any civilian hackers or doing any hacking themselves. However, China does admit that their country's intellectual property system still lags behind developed countries and needs improvement. "China still lacks legislative experience on intellectual property protection, and enterprises don't have enough consciousness to protect themselves from pirates by appealing to the law," said Zhang Qin, deputy director of State Intellectual Property Office. In October, China's Commissioner of State Intellectual Property Office and the director of the United States patent and Trademark Office signed a Memorandum of Understanding on a desire for cooperation, but where exactly this will lead is uncertain.<sup>8</sup>

It should be noted that China and Russia are hardly the only countries that are sources of threats to US IP. IP threats can and often do originate in countries that are considered friendly allies. Companies in every country that compete with US companies are interested in US IP and citizens and companies in many of these countries are also potential IP threats for US companies. In addition, IP threats can and do originate in a company's home economy as well. Thus, it very important for companies to develop and

---

<sup>6</sup> See, <http://www.foxnews.com/politics/2008/11/20/pentagon-cyber-siege-unprecedented-attack/> 11/20/08.

<sup>7</sup> See, Epstein, Keith. "The taking of NASA's Secrets." *Business Week* December 1, 2006. pp 73-79.

<sup>8</sup> Intellectual Property Protection in China, November 2008. [www.chinaipr.gov.cn](http://www.chinaipr.gov.cn).

**implement policies and procedures against theft or loss of proprietary IP. The next section outlines some illustrative practical approaches used by large and small US companies to protect their IP assets.**

### **How Should a Company Respond to these Threats?**

**First, stay calm. According to Mr. Petras, it is important to remember that the threat of imitation and reverse engineering is not new. During the middle to late industrial revolution, England complained about American companies copying their goods and selling them back to England cheaply, forcing many English companies out of business. Currently, there are many companies in the U.S. that reverse engineer products to discover secrets and determine how they can make a competing product. The key is to stay steps ahead of your competition. Mr. Petras advocates using answers to four important questions to guide IP strategy: 1. How can this be copied/infringed? 2. Who would want to copy/infringe it? 3. Why would they want to copy/infringe? And, 4. What can you do to prevent copying/infringement?**

**At a minimum, a company needs to institute available legal protections and determine where you want to protect it. IP is essential when a company wants to establish or come into a market, according to Ms. Diane Dominick from the Steris Corporation. The original idea that formed Steris was a table top sterilizer for endoscopes. The inventor was told this idea would never work, but he foresaw the increased used of endoscopes as surgery continued to get less invasive. By securing IP rights, Steris secured a market position and has grown from 5 employees to over 5,000 employees and more than \$1 billion in revenue.**

**When moving into an international market, the first step Steris takes is registering its Trademark (TM). Its policy includes filing in the US, in markets that could potentially be profitable and any other strategic locations. As Mr. Petras noted, this provides important protection for market recognition. He once faced a situation where a client got a call from someone saying “I want to be your distributor in Uruguay, and by the way, I own your TMs here.” This is why a company needs a comprehensive plan from the start.**

**Sometimes, a company needs to be creative. For example, there are many illegal copies of Microsoft Windows in China. To battle this, Microsoft has launched a “screen Blackout” anti-piracy program. This involves software that Windows will automatically install on a computer. If the copy of Windows fails the validation test, their will be hourly desk top blackouts and permanent pop-up notifications in efforts to persuade users to switch to a genuine copy. Microsoft’s goal is “helping [people] get a genuine Microsoft product because they sometimes may not know they have paid for a fake one” according to an executive with Microsoft China. Microsoft will be using this strategy in other markets too, in an effort to alert users but not prevent them from using their**

**current computers. Whatever a company's method, it is important not to anger your consumer base unnecessarily by an anti-counterfeiting campaign that is seen as overbearing.**

**To be sure, some chief executives are getting it right, usually after getting a swift kick from the market. Mal Mixon, CEO of Invacare, a \$1.5 billion medical product manufacturer and distributor in Elyria, Ohio, remembers when he bought the company 25 years ago. "In the first 20 years, I didn't pay that much attention to patents," he says. "Part of the reason is that we were beating people pretty easily. We filed for patents, but we weren't as serious as we are now." Not only does Invacare have domestic competitors, but also many knock-off imports from China with prices 30 to 40 percent less than Invacare's. "We have a competitor that actually copies the parts numbers and makes them interchangeable with [ours]," Mixon says.<sup>9</sup>**

### **Developing an Internal Plan of Action**

**All employees need to be familiar with this comprehensive plan. Diebold uses a "best practices" approach to IP protection and management. Ms. Jackquelyn Strickland of the Diebold Corporation describes this process as starting with people. Your workforce needs to be educated about company policy. Train employees from the first day. Each employee should sign an agreement to assign rights of any invention or other created IP to your company and to respect the IP of other companies.**

**Employees need to be positively reminded about company policy. This can be accomplished by encouraging innovation and reporting of new ideas by employees. Also, companies need to engage IP counsel from the start of the process. This way decisions, such as, "do we need to patent/TM an invention?" are made before the IP is accidentally put into the public domain. In addition, you need to have an exit policy for employees that leave, dealing with nondisclosure, inventions and trade secrets.**

**In addition, it is important to be aware of the laws of your state regarding IP rights. Some states, such as California, have liberal laws where an invention/idea has to be reasonably within the scope of employment for a company to claim rights. In Silicon Valley, people are constantly creating new companies with technology they may have thought up at a previous employer. Similarly, as Dr. Aggarwal notes, while the Geneva Act has not yet been implemented in the US, many countries have adopted it and there is some case law in the US consistent with this act to protect designs of commercial products (17 USC 1301-1332, 2005) initially for two years which can then be extended for another ten years.**

---

<sup>9</sup> Chief Executive, November 2004.

**Be careful with trade secrets, as they can be a vital asset of a company, in the US and abroad. Ms. Strickland describes them as including information on customers, methodology, algorithms, and how you manage your IP process. If a legal matter arises concerning a trade secret, your company will have to prove you treated the trade secret as a trade secret by showing a cradle to grave processes. For example, in China domain names are often copied. The Asia-Pacific region always is a challenge, but one has to find out about infringements first before you can act. And as Dr. Aggarwal notes, it is important to keep key aspects to a few people to limit the chance of the secret getting out.**

**This internal plan of action is important not just to protect against foreign countries or competitors, but to protect yourself from your own employees. Kyung Kim, who received doctorate in physics from the Rennselaer Polytechnic Institute in New York, sold Lubrizol Corporation secrets to a competitor in South Korea. He was recently sentenced to 19 months in prison and was ordered to pay \$188,700. According to the Cleveland *Plain Dealer*, Kim felt like a failure because of his lack of advancement, perceived lack of respect at work and a failed marriage.<sup>10</sup> This combined with greed led him to sell the secrets. This incident illustrates the need to educate employees on policy and disciplinary procedures. Also, there is a need to check on how employees with confidential information handle these secrets and limit an employee's knowledge to what he or she needs to know to complete his or her duties.**

**Indeed, as Dr. Aggarwal noted, it is very important that a company view IP as a real business asset (even though it is an intangible) and develop a corporate wide culture of protecting IP assets. These efforts have to start with senior management who only can set the tone and provide adequate motivation to build IP protection in corporate culture. Corporate culture is perhaps the most effective means of IP protection given that explicit controls are difficult to implement and enforce when trying to protect intangible assets.<sup>11</sup>**

### **Exercising Healthy Paranoia**

**Preparing for the worst can be the best plan. Mr. Donald Esarove, President of the Cypress Corporation suggested that whenever dealing with “proprietary property” (PP), think “healthy paranoia” (HP). Be cautious whenever anyone inquires into your business process, product specifications, or customer/vendor lists. Be aware of the reality that if you are successful, someone will try to knock it off, so your company needs to make their PP difficult to copy. For example, if you have an overseas vendor who wants to**

---

<sup>10</sup> [http://blog.cleveland.com/metro/2008/11/lubrizol\\_corp\\_worker\\_gets\\_pris.html](http://blog.cleveland.com/metro/2008/11/lubrizol_corp_worker_gets_pris.html)

<sup>11</sup> For additional details, see for example, Dobrusin, Eric M. and Ronald A. Krasnow, *Intellectual Property Culture* (New York: Oxford University Press, 2008) and Arena, Christopher M. and Eduardo M. Carreras, *The Business of Intellectual Property* (New York: Oxford University Press, 2008).

**know your entire process – this should be a red flag. Do not disclose the whole process to them as they generally do not need to know all of it. Instead, let vendors supply only certain components especially in foreign countries that do not provide much legal protection, “when dealing with PP, use HP”.**

**This may be as simple as separating where key components are made and/or limiting workers knowledge to certain aspects of the process. Since mechanical equipment can be reversed engineered quickly, once you commercialize it then people can copy it. If your device is obvious, think about a TM for your brand name. Dr. Aggarwal notes that protecting your market position is the key. You may want to promote why your brand is better than the competitors/counterfeiters – “the original”, perhaps due to superior quality and/or post-purchase service. Also, for smaller companies, Mr. Esarove advises looking for a big partner but remember to get a non-disclosure agreement before you enter into any talks. Once your product hits the market place, you are naked, but the large company partner can help get you into more markets quickly, while protecting you along the way.**

**In addition, watch out for patent trolls. Patent trolls are people or groups that file a patent or purchase patent rights not to produce a product, but to sue infringers. This often arises in the pharmaceutical areas, according to Mr. Petras. As a result patent portfolios do not mean as much as it used to. The key is to be aware of patents that others might own. Your company may even have to do some creative designing of its own as protection from trolls. By focusing on company procedures, quality patents, and getting rid of ones you do not need, your company can strengthen the value of its IP portfolio. Business method patents are another major threat to corporations today and a popular way for patent trolls to work their strategies. While the current patent system is very liberal in allowing method patents, recent policy re-considerations may force a constricting change in method patents in the near future.**

### **Conclusions:**

**This paper has provided a brief overview of why it is important to protect intellectual property and it has argued that policies and procedures for such protection should start with management practices and not just with legal actions. Indeed, it is usually not cost effective to use legal protection as the first line of defense.**

**There are many sources of domestic and foreign threats to IP assets. In fact any national or commercial competitor can be a source of these threats. Protection of IP assets is a critical task for corporate managers and it is important to develop and institute appropriate policies and procedures throughout the company to protect IP assets. This paper provided a framework to think about these issues and detailed many practical examples of such policies and procedures that can be adapted for use in US companies.**