IP Protection in a Borderless World

Today's dynamic international trade environment and mosaic of national regulations make intellectual property protection as complex as it is important.

Guarding against IP theft is a priority of 72 percent of the respondents to this year's *Global Fraud and Risk Report* survey. Furthermore, 43 percent name it a *high* priority, which means that, overall, respondents assign IP theft an urgency second only to that of data theft. Our survey shows that this concern is warranted: 24 percent of respondents said their organizations experienced a significant incident of IP theft within the last year, up from the 20 percent reported in the 2017–2018 survey.

THE ARRAY OF THREATS

Survey respondents identify a range of perpetrators of IP theft or misappropriation. Competitors, contractors, employees and third parties (such as joint venture partners, vendors and suppliers) are each responsible for approximately one-fifth of the reported incidents. The wide variety of perpetrators underscores the many ways in which IP theft or misappropriation occurs.

Contractors and employees, for example, respectively account for 19 percent and 18 percent of IP theft. Perpetrators from these groups often commit IP theft by taking confidential information with them when hired away by a competitor, or by engaging in espionage, selling the company's secrets to its rivals. Motives abound: The employee or contractor could have been disgruntled, bribed or even secretly employed by a competitor all along.

Seventeen percent of IP incidents arise from **third parties**, such as joint venture partners, suppliers and vendors. Without proper safeguards, business partnerships and supply chain relationships can bring IP risk because they are generally predicated on sharing sensitive information. This risk warrants particular focus when these relationships cross borders, as is increasingly the case in today's globalized economy. Enforcement in response to IP theft can be challenging and should be given ample attention when developing the partnership terms. Patents and trademarks offer protection only in the jurisdiction where they are issued, and trade secrets and proprietary know-how don't have the same legal protection across jurisdictions from competitors, foreign governments, employees and other bad actors. The effectiveness of enforcement varies among countries as well. The resulting patchwork of protection makes any IP holder particularly vulnerable to theft or infringement when its supply chain, operations or distribution networks extend to foreign countries.

This vulnerability may be increased further by a country's policies on foreign investment. One area of tension between the United States and China, for example,

CHRIS BAKEWELL

Managing Director
Disputes
Houston, TX, US
chris.bakewell@duffandphelps.com

PAUL BENSON

Director
Disputes
Minneapolis, MN, US
paul.benson@duffandphelps.com

TAD KAGEYAMA

Regional Managing Director, Asia Pacific
Business Intelligence and Investigations
Singapore
tkageyama@kroll.com

has been "forced" technology transfer arising from Chinese regulations that make it very difficult for a foreign company to operate in China without partnering—and thus sharing its IP with—a Chinese company. China recently introduced legislation that would ease foreign investment rules, but only time will tell if this change will have a meaningful impact on this deep-rooted conflict. Intellectual property is a key issue in U.S.–China bilateral trade negotiations, and it will be important to see what, if any, terms are agreed to.

Competitors account for 21 percent of reported IP theft incidents. While such incidents can arise from deliberate actions such as direct infringement, espionage or reverse engineering, indirect infringement also can be a common problem, especially because it can occur inadvertently. Consider a scenario in which a German company contracts with a Taiwanese firm to manufacture a medical imaging device according to a particular design and set of specifications. In manufacturing the device, the Taiwanese firm uses a technology for which a rival medical imaging company holds the German patent, and for which the German company does not have a license. The German company might risk infringing on the rights of the patent-holding competitor as soon as it distributes the device in Germany—and without proper planning, may not even know that it is doing so. Investigating, managing and measuring the impact of these issues can be challenging, and organizations may find it beneficial to have their plans reviewed by third-party specialists.

MITIGATING RISK

To mitigate against IP-related risks, companies can take several steps. A company's first step is to make sure it is taking adequate precautions to **protect its IP within its own facilities**. After all, employees and contractors together were responsible for 37 percent of the IP theft incidents reported in our survey. Access to intellectual property should be restricted and monitored, and then promptly revoked upon an employee's termination or resignation. Management should develop policies to address which personnel have rights to access IP and then monitor access to ensure compliance. Such policies should also address and limit any potential to copy or distribute the company's confidential information.

Secondly, organizations that establish IP sharing agreements with business partners, suppliers and manufacturers should **consider a defensive mindset** when drafting the appropriate contractual safeguards. For example, contracts need contingencies to address a counterparty's potential acquisition, whether a license granted to the counterparty extends to the counterparty's subsidiaries, and the counterparty's right to sub-license the IP; the terms of such an arrangement should be crafted so as to consider, and possibly prevent, the counterparty licensing the IP to competitors. Companies sharing IP with third parties need to specify the physical and cybersecurity measures under which the counterparty must hold the intellectual assets, such as access-restriction policies and the encryption of sensitive information.

FIGURE 14

WHO ARE THE PERPETRATORS OF IP INCIDENTS?

Thorough due diligence is also crucial. Examining a company's financials and performance track record is not sufficient; proper due diligence will include business conflicts and litigation involvements of the entity, its management and its board members. The process should also involve investigating the counterparty's ability to execute and maintain the specified security procedures.

When third-party relationships cross borders, organizations should step back and **map the local IP landscape**. This means understanding not only the IP regulations and protections in each country, but also each country's effectiveness in enforcing its protections, and the capacity, disposition and transparency of its courts in handling IP matters. All of these factors determine, in practical terms, the company's level of recourse should infringement occur. To the extent possible, appropriate clauses addressing these factors should be incorporated into any license agreement or business partnership. A holistic view of the entire IP strategy—including enforcement, licensing and monetization scenarios—is essential to informed decision making and preparation. The counsel of an experienced local law firm is also essential to incorporating this strategy into agreements.

A country's IP landscape includes the places where IP protection intersects with the government's **foreign and domestic policy**. This includes such issues as the restrictions on foreign investment discussed above, as well as any history of compulsory licensing, including situations in which the government essentially allows local companies to selectively infringe on foreign patents. These infringements may be permitted by the government under the cover of advancing a public good, such as improving access to healthcare. Take special care when entering into IP-sharing agreements with state-owned enterprises, which may have a local advantage in the adjudication of any conflict that may arise.

Finally, if there is **the potential for theft or infringement**, that risk needs to be thoroughly assessed and incorporated into the relevant business decision making.

WHEN INFRINGEMENT OCCURS

Regardless of how carefully a company might work to mitigate its exposure to IP risk, unfortunately, infringement and theft do occur. When that happens and legal action ensues, the strength of the case will rest on how compellingly the company can demonstrate actual harm. The complexity and global nature of the typical company's operations and supply chain often make this a challenge. The effort is usually shepherded by the in-house legal department, working with outside counsel to provide expertise on the type of IP theft or misappropriation and on the jurisdiction in which the company is pursuing legal action. Other professionals can provide important input as well. Economic experts, working with technical and marketing experts, combine industry expertise with qualitative and quantitative intelligence to assess and quantify the damages inflicted by the infringement or theft. Doing so may require, for example, isolating the incremental value of the intellectual property in question, and then quantifying the economic harm resulting from the wrongdoing. Constructing these economic arguments calls for a team with deep understanding of IP disputes, acute analytical skills, and experience in addressing the full range of relevant issues and potential IP damages.

LOOKING AHEAD

The impediments that arise from the wide range of national approaches to IP protection and enforcement have motivated many companies to attempt to establish a global approach to intellectual property. However, regulatory differences among jurisdictions make doing so difficult. Understanding the impact of reform efforts in individual countries—China, Brazil, and India among them—will form a basis for a global framework. There is now broad awareness among countries that sufficient and reliable IP protection is a powerful differentiator in the competition for foreign investment. The increased attention paid to IP issues in bilateral trade agreements is another factor to monitor and assess. Regardless of whatever advances may be made, companies must continue to be alert to the range of IP risks and be prepared to integrate the appropriate mitigations into both their IP monetization strategies and their operations.

> Any potential for IP theft or infringement needs to be thoroughly assessed and incorporated into business decision making.