TREASURY & RISK
THE FUTURE OF FINANCE TODAY
An ALM Publication
FEBRUARY 4, 2021

Mitigating Losses from Intellectual Property Theft

IP threats are on the rise. Here's how to protect your company's "golden goose."

BY RANDY SADLER

When companies consider theft risk, they're usually analyzing threats to their physical assets or the chance a rogue employee will engage in embezzlement. But sometimes the biggest, most detrimental loss a company could face is intangible. Intellectual property, or IP, refers to creations of the mind. Many IP assets are protected under law as copyrights, trademarks, or patents. Other forms of IP can include trade secrets, manufacturing processes, and other know-how that is difficult for competitors to replicate.

For treasury departments in companies that rely heavily on IP to generate value, protecting intellectual property may be as important as protecting cash flows and leading corporate investment strategy. After all, for many businesses, IP is the goose that lays golden eggs. Wise treasury professionals keep an eye on all the company's golden eggs and take active measures to shore up the source of each egg.

IP Theft in the Headlines

Companies face substantial losses as a result of IP theft. The Commission on the Theft of American Intellectual Property estimates that annual costs from IP losses range from $225 billion to $600 billion. It's also worth noting that the loss of IP is different from other types of loss. Stolen or damaged inventory or vehicles can be replaced through insurance, but the effects of stolen IP truly cannot be canceled out. IP infringement may rob a company of revenue and put downward pressure on its prices.

Consider what happened to American Superconductor, a Massachusetts-based provider of clean-energy solutions. In 2011, American Superconductor's largest customer, China-based Sinovel, ignored the companies' contract and refused to pay millions of dollars it owed. American Superconductor then discovered that Sinovel had obtained the source code for its electronic components and was installing a pirated version in wind turbines. The violation of American Superconductor's IP rights and loss of revenue from Sinovel reduced American Superconductor's revenue by $100 million per year.

In cases like this, there is no possibility of recovering stolen goods. The victim company's only recourse is to wage a legal war to block the thief from using what they've stolen. This is always challenging but becomes even more difficult when the thief is foreign. At a minimum, the IP owner can sue to block the thief's access to the U.S. market and protect some of its rights and revenues. Then the business can make decisions on whether to wage legal battles in other countries—or simply choose to compete head-to-head with the unethical competitor overseas.

For companies that rely on intellectual property as their primary differentiator, protecting those IP assets is a business-critical task. In trade talks and news stories through 2019 and early 2020, China's intellectual property theft was a trending topic. A **CNBC CFO survey** found that China had stolen intellectual property from one in five corporations within the previous year. Moreover, a **2015 paper by the Federal Reserve Bank of Minneapolis** concluded that more than half of all technology owned by Chinese firms was obtained from foreign companies.

This has been going on for decades. In a **2007 example**, customs agents at O'Hare International Airport in Chicago stopped Motorola engineer Hanjuan Jin. They found she was carrying $30,000 cash and a bag full of confidential and proprietary Motorola documents—along with a one-way ticket to Beijing. Jin, who was born in China, was a successful engineer working on Motorola's cellular technology. Investigations revealed she had taken a medical leave in 2006 to go to China, and in violation of her Motorola employment, she had pursued a job with Sun Kaisens, a Chinese telecom company. When she returned to work for Motorola in Chicago, she was seen leaving the office with bags full of documents in the evenings. She was later found guilty of intellectual property theft and sentenced to prison.

In March of 1992, the head of the Business Software Alliance, a group that includes major software companies, found that its members had lost $225 million in software sales in China through piracy of music, videos, and software.

Options for Protecting the Goose

So, how can companies that depend on IP—like American Superconductor, Motorola, and thousands of others—prevent the financial fallout from IP theft?

Certainly, there are measures organizations can take, including stiffening cybersecurity practices, developing an inventory of intellectual property and then carefully tracking each asset on the list, limiting information access to the individuals who truly need it, and utilizing data loss prevention software. Companies can also strengthen legal protections for their IP by registering additional patents. This approach makes it more difficult for competitors to engineer knockoffs and copycat products.

Companies should also enforce strict internal security policies and carefully vet job candidates. Having the right people and processes in place is critical. However, even with the right processes in place, IP theft is a complex, ever-changing threat that can occur unexpectedly. And when it does, the die is cast. It's often an "all or nothing" struggle to stem the loss or suffer major defeat.

Another backstop to protect against IP theft is purchasing a commercial insurance policy. In fact, this is becoming an increasingly popular solution, with IP insurance growing at a rate of 300 percent annually, according to an article by the International Risk Management Institute. This type of insurance covers the legal costs of an IP-related lawsuit and any resulting settlements or adjustments. The insurance can also cover the cost of pursuing other companies that infringe upon the insured business's IP rights.

Evaluate the Risk

Companies looking to protect their intellectual property must address five critical issues:

1. ***What are the ways in which our IP (protected by a patent or trademark) could potentially be compromised?*** In each of those envisioned events, would a court agree that our legal rights were violated? Would an insurer agree that our trade secrets were stolen?

2. ***Could the damage be minimized through legal means?*** This might include filing an injunction to stop the encroaching company until the matter's resolved. If the theft of trade secrets could not be addressed legally, could it be addressed by other means—and what are they?

3. ***Would a compromise cause real financial loss?***

4. ***How could the loss be measured?***

5. ***Are there ways in which the company could mitigate or address the loss?*** For example, would insurance pay for the legal costs to stop a patent infringement? Would insurance pay all or a portion of lost revenue due to the theft of trade secrets?

Understanding the answers to these questions across the company's different IP vulnerabilities enables the treasury team to not only quantify the potential financial impact of IP theft and loss, but also identify specific threats. Knowing how it might be compromised helps the company plan more effective IP protection.

Captive IP Insurance

Treasury departments looking to prepare for the unexpected may also want to amass a stockpile of cash. One financial vehicle that can simultaneously help protect the IP "golden goose" and build cash reserves: The business can form and own a captive insurance company that supplements its purchased commercial IP insurance.

The corporate treasury group may be called on to invest a captive's loss reserves... Over time, it's possible for a captive to become a profit center.

A captive insurance company is a wholly owned subsidiary that issues insurance policies to protect the parent company. The company pays premiums to its captive insurer, and the captive operates very much like a commercial insurance company. Its policies are underwritten and priced by an actuary. The captive maintains loss reserves; the actuary determines the appropriate size of loss reserves based on insured risks, and the domicile regulator approves the loss reserves. Because they are licensed insurance companies, captives can access reinsurance markets to backstop the coverage they are providing.

In the event of an insured loss, the parent company can file a claim with its captive insurer. A claims administrator will verify that the claim is real and insured, and will approve it. The captive will then pay the claim to the business.

The corporate treasury group may be called on to invest a captive's loss reserves. It's important to note that captives can defer taxes on loss reserves, enabling accumulation of a larger pool of funds for investment. Incoming premiums that aren't paid out as claims or in administrative costs further increase the size of the loss reserves or become underwriting profit. Over time, it's possible for a captive to become a profit center.

Captives can write broad coverage for IP losses, to insure gaps in commercial policies. Still, although there are no regulatory or legal restrictions on the way a captive formulates its IP policies, the captive must clearly define what a loss is, losses most be economically measurable, and insurance contracts require fortuity—in other words, when the policy is written, there must be uncertainty about whether a loss will occur, and the possibility that no loss will occur.

If an IP theft results in losses that are covered by commercial insurance, the company can file a claim. If the losses are also covered by the captive (possibly as an excess policy), the company can file a claim on its captive as well.

In some cases, an IP loss may not be covered by commercial insurance, but may be covered by the captive. For example, a commercial insurer might argue that a company's patents or trademarks have not actually been infringed, or a commercial policy might have exclusions for some types of IP theft, such as theft by an employee. Alternatively, some IP losses—particularly those that fall into the category of "trade secrets," as opposed to patents or trademarks—may not be insured by either commercial insurance or the captive. In these instances, the treasury or risk management team that manages the captive can come to the rescue: The captive can pay a large dividend to the company to address the loss, or—in extreme cases—the captive's policies may be canceled, and the captive can be liquidated to pour needed cash into the company.

A Step-by-Step Approach for Protecting the Golden Goose

Crafting a risk management strategy for IP theft is critical, and this responsibility will often fall on treasury or require significant input from treasury. The stakes are high. Would-be IP thieves are tireless. And there is no shortage of companies willing to rip off someone else's intellectual property, or to develop a patent-skirting knockoff that necessitates a legal fight. This is not the place to cut corners. In fact, for businesses that are highly reliant on IP, it is reasonable to allocate a sizeable share of the company's golden eggs to protect this goose.

The first step for a treasury or risk group looking to protect the company's intellectual property is mitigation. Be diligent and thorough in the hiring process. Going back to the 2007 Motorola IP theft example, employees can play a role in the theft of IP so integrity is critical.

The next step is to ensure that the company is adequately insured against IP theft. Insurance can be costly and difficult to acquire, but even a low-limit policy can fund a legal challenge, should it be necessary to protect the company's revenue stream.

Finally, organizations ready for a more advanced IP protection strategy should consider forming a captive insurance company to provide both depth and breadth to the IP defense plan. Captives offer flexibility, which can be critical to treasury and risk teams charged with protecting the organization's "golden goose."

Randy Sadler *started his career in risk management as an officer in the U.S. Army, where he was responsible for the training and safety of hundreds of soldiers and over 150 wheeled and tracked vehicles. He graduated from the U.S. Military Academy at West Point with a B.S. degree in International and Strategic History with a focus on U.S.–China relations in the 20th century. He has been a principal with CIC Services, LLC for seven years. In this role, he consults directly with business owners, CEOs, and CFOs on the formation of captive insurance programs for their businesses. CIC Services manages more than 100 captives.*