

DISCLAIMER: This document is provided for educational and informational purposes only and is not intended and should not be construed as providing legal advice concerning Intellectual Property rights. The views and opinions expressed in this document do not necessarily state or reflect those of the U.S. Government or the private sector partners participating in the Public-Private Analytic Exchange Program.

Intellectual Property Rights

Public-Private Analytic Exchange Program Research Findings

Scope

The Intellectual Property Rights (IPR) Team, a group of private and public-sector participants in the 2017 Public-Private Analytic Exchange Program, researched the opportunities and risks associated with Intellectual Property (IP) throughout the innovation and product life cycle. The team broke down the cycle into the following stages: Research & Development; Manufacturing & Testing; Sales & Marketing; Supply Chain & Distribution; and Financial Gains & Sustainability. This is a report of the research findings of the group. It is not intended to be a comprehensive look at all IPR-related issues, but rather focuses on some of the most essential issues that both start-up and mature businesses may want to consider in protecting IP, as well as some of the emerging threats and opportunities posed by technological and marketplace change.

Intellectual Property Rights

The economic success of the United States is dependent on the ability of the private sector to innovate and the marketplace to remain competitive. While there is no formula for a successful company or product, the intellectual, or intangible, assets of a company often represent the ‘secret sauce’ or differentiating factor that drives success. Intellectual Property has been valued and protected since our country’s founding, as evidenced in the U.S. Constitution: Article 1, Section 8, Clause 8 gives Congress the power to “*promote the progress of science and useful arts, by securing, for limited times, to authors and inventors, the exclusive right to their respective writings and discoveries.*”

The value of IP and the opportunities for economic prosperity and collaboration inherent in it are immense and worthy of protection. When IP is taken or exploited, IP owners can incur losses and can be disincentivized from further development. IP can benefit from legal protections through a system of intellectual property rights (IPRs) that vary by country or can extend across borders as part of certain trade agreements. IPRs detail the legal standards by which the ownership of original knowledge is defined, recorded, and valued. These standards give intangible assets the same basic characteristics as real or tangible property. IPRs do not, however, prevent intellectual property rights from being violated, and steps must still be taken by IPR owners to protect and defend their intellectual property.

Key Findings and Approach

The IP Rights team found that the vast majority of risks and opportunities identified in the literature and in interviews with industry and government experts apply to each and every stage of the product life cycle. This document details key findings and insights from the team’s research, first looking across the commonalities, followed by a review of each stage in the product life cycle, and concluding with some actionable take-a-ways. Those key findings can be summarized as follows:

- **Devoting resources for *proactive* measures that can protect IP may not be a top priority of many businesses, perhaps especially start-up and small businesses, resulting in a *reactive* stance after IP rights have been violated. Our work identified numerous proactive measures that businesses can take throughout the product life cycle to prevent IP from being stolen and exploited, including legal, physical and digital security measures, and other efforts such as employee and consumer education. These measures can help turn risk into opportunity, and positively impact firm value.**
- **The current business environment reflects rapid technological change, development of a global marketplace, decentralized R&D, and a shift in firm value from tangible, physical property to intangible, intellectual property. The introduction of 3D printing, cloud computing, and the Internet-of-Things (IoT) are amongst the most prominent new technological developments. Collectively, these environmental changes have shifted the risks and opportunities associated with IP.**

Managing Risks to Maximize Opportunities across the Product Life Cycle

Regardless of the stage a product is in, risks exist that can lead to IP rights violations. There are a range of solutions that can help mitigate these risks, as well as provide opportunities for companies. Mitigation strategies are discussed within three categories: legal measures, physical and digital protection, and human resource measures.

- ***Legal Measures.*** Corporate legal activities can assist with enforcement and civil litigation actions taken by or on behalf of IP owners. Taking legal steps in advance of an incident can be a necessity to preserving IP rights in a court of law. Legal protections can also be used as a key deterrence and to signal other parties that the rights owner believes their IP is valuable and worth defending.
 - ***Non-Disclosure Agreements.*** One of the easiest forms of legal protection an individual or company can deploy is a non-disclosure agreement. Non-disclosure agreements (“NDA’s”) should be employed whenever a protectable idea or research is disclosed to researchers, investors, collaborators, vendors, or employees. NDA’s give the IP owner certain legal recourse should the counterparty misuse the information disclosed to them in confidence. NDAs can also define company ownership of IP and IP rights.
 - ***Patents, Trademarks, and Copyrights.*** Legally protected forms of IP include copyrights, trademarks, and patents. A copyright can protect original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture. Patents on the other hand protect inventions or discoveries. Trademarks protect words, phrases, symbols, or designs identifying the source of the goods or



services of one party and distinguishing them from those of others. Taking steps to file and register for these protections does have a cost but can be essential to monetizing certain ideas and inventions.

- *Trade Secrets.* Trade secrets, a category of IP that does not require formal registration, can also have real value to owners. Trade secrets include information, such as a formulas, patterns, processes, or compilations of data otherwise unknown to the public that is used by a company or embodied in a product. Once known to the public, a trade secret is no longer a secret and no longer enjoys the legal benefits of trade secret protection. Owners do not enjoy exclusive rights to their trade secrets should others develop similar capabilities on their own. Although registration of a trade secret is not required, owners must take steps to secure and defend these secrets.
- *Vendor Compliance.* Vendors and other third parties that have access to company IP resources should be held accountable in the event of a loss attributable to their action (or inaction). Compliance and programs that assist vendors in meeting the security expectations of the company are common.
- *Physical and Digital Protection.* Legal measures on their own do not necessarily provide for mitigation for IP violations. Physical and digital measures go more directly to reducing the risk of loss.
 - *Cybersecurity.* Almost all IP today takes an electronic form and the protection of electronic documents and data is important. Basic cyber hygiene, such as disabling USB drive access for certain computers and employees, monitoring mass downloads of information, updating computer software to protect from the latest cyber exploits, and installing data loss prevention agents will help. Two-factor authentication on computer systems, complex passwords, network access logs, and encryption are a few examples of tactics that can be employed by companies.
 - *Physical Security.* While the focus is most often on cybersecurity, physical security remains an important component of any IP security plan.
 - *Regional Issues.* IP protection varies by country and it is inherently difficult for companies to protect IP when it resides within certain jurisdictions. IP violations are also more prominent in certain countries like China, Russia, India, and Mexico. Companies can implement specific IP protection strategies when employees reside or travel to these and other high-risk countries or regions, including the use of new computers that contain only specific data required for the trip, preventing corporate network access, and specific education efforts aimed at travelling employees.
 - *Cloud Services.* The use of online and cloud-based services can be productive and cost effective for companies from a data storage perspective as well as with value-add services such as customer-relationship management (CRM) systems that help companies maintain and organize important and often proprietary data. Companies should understand the security of any external system, as well as have a clear understanding of where (geographically) data is



stored, its availability in the event of a vendor default, and if the third-party retains any IP rights for using or sharing on their platform.

- *Data.* Advances in how we move and store data (and how much of it we can and do frequently move and store) have fundamentally shifted the burden of protecting against IP violations from inside a company, to both inside and outside. The long chain of freelancers, software developers, test audiences, product reviewers and “beta” users means that companies need to take extra security precautions.
- *Human Resource Activity.*
 - *Leadership.* The protection of IP should start at the top level of a company, mandated by the Board of Directors and Shareholders and implemented and lead by company management. The CEO, CFO, and the Chief Security Officer, amongst others, should understand the company’s IP inventory and what its value is to the company (and to competitors and would-be thieves).
 - *Employee Education.* All corporate divisions from HR, marketing, sales, legal services, production, and R&D can pose a risk for IP loss. IP disclosure often occurs accidentally by employees, irrespective of the level of employee in the company. Additionally, employees often inadvertently facilitate cybersecurity breaches. Educating employees about the importance of protecting IP, phishing/pharming, abusing IT systems, errors/omissions, employee telework procedures, and/or using mobile devices to conduct company business, can help.

Stage 1: Research and Development

The Research and Development (“R&D”) phase is the critical first phase of a product or service that spans from the idea phase through to the development of an actual product or service ready to be built and marketed. Given the significant cost associated with R&D, even established companies have come to utilize outsourced and decentralized R&D under certain circumstances, further increasing the footprint of IP risks.

- *Early Stage IP.* The R&D stage sees the emergence of significant intellectual property (“IP”). Even the development of tangible property and corporate operations start with proprietary research and analysis that may be protectable in the form of trade secrets or patents. How emerging IP is handled within a company can be critical to its viability as a commercial entity.
- *Collaborators and Investors.* The R&D phase for a company can expose early stage IP to a wide group of individuals—collaborators and investors. Collaborators and peers are important to ‘trying out’ ideas and investor money is important to commercializing the ideas. These parties will conduct sufficient due diligence to gauge their respective investments in time or money and may force companies to disclose details of IP. While NDAs apply at each stage of the product life cycle, they are especially important during the R&D phase. The NDA can help with real legal recourse in the event of exploitation. Perhaps more important, at this early stage, the NDA sends a signal of deterrence and a signal that the company values its IP and takes its protection seriously.



- *Licensing and Sale Opportunities.* A hallmark of the R&D phase is that very few ideas ultimately get through this initial phase successfully, despite significant investments of time and money by individual entrepreneurs and corporations. IP value varies significantly depending on who owns or has rights to the IP. Companies may still find unutilized IP is worth protecting and may find sale or licensing opportunities.

Stage 2: Manufacturing and Testing

Manufacturing has increasingly become a commoditized activity. Manufacturing equipment was once very unique, cumbersome, and extremely expensive whereas today, products are often easier to manufacture *en mass* and developments like 3D printing can see a product being produced by virtually anyone that possesses the required electronic design file. Manufacturing was also once carried out close to the point of sale, but shipping costs have become much more competitive and products can now be manufactured anywhere in the world.

- *Counterfeit Manufacturing.* Sophisticated manufacturing technology is being used to produce infringing products across all industries. These counterfeit products resemble genuine products so closely that they are, to the naked eye, indistinguishable from the genuine products, and in many cases are only detectable via the use of secondary or expert examinations.

The proliferation of counterfeit products is no longer limited to luxury consumer products like handbags and watches, it now applies across all industries to include pharmaceuticals and pesticides, food products, and electronics. The counterfeiting of products in new industries poses new risks, including health and safety risks. These risks in turn can threaten the viability of entire product segments. Also, to the extent manufactured counterfeits represent components used as inputs to other products, the ultimate product can pose a significant liability for consumers and companies.

- *Electronic File Risks.* Manufacturing processes are increasingly automated and more dependent on computer guidance. There are two primary ways in which this poses a threat. First, the blue prints to the process, once in paper form on the factory floor, are now typically stored electronically and vulnerable to cyberattack. This includes files that guide the machines used in both traditional and additive (3D) manufacturing. Second, manufacturing processes utilize sensor technology and the Internet-of-Things (IoT) to capture data and fine tune the manufacturing process. This can include detailed adjustments that would have been known only to individual craftsmen in a factory. While the risk of cyber breach and the theft of electronic data is certainly not unique to manufacturing, the risks posed to manufacturing are relatively new and cannot be overlooked.

Stage 3: Sales and Marketing

During the sales and marketing phase, the details of a product are often first provided to the marketplace. Companies and illicit actors conduct research to understand how to recreate or otherwise compete against products.

- *Electronic Data Theft.* Copyrighted material stored in electronic format can be vulnerable to pirating during the sales and marketing phase when products first become exposed to consumers. For example, the movie industry typically keeps its content in electronic format. During the marketing phase when movies are screened and reviewed by the peer community, digital copies and even links to online copies, can be given out. During the sales process digital copies or links are sent to movie theaters. Unless careful tracking and logging of use is performed, illicit use can lead to strategic failure of product launch and the suppression of legitimate sales.
- *Elicitation of Proprietary Information (PI) or Social Engineering during Sales Conversations.* Sales and marketing employees are focused on bringing attention to products/features and ultimately making sales. Often employees with intimate knowledge of IP and trade secrets are also involved in the selling process. The difference between proprietary information and marketing information available for use during sales presentations must be well defined and known to anyone communicating with customers.
- *Brand Impact.* The sale of counterfeited goods can harm brand reputation and value across an entire industry or product category. Investment in consumer awareness of counterfeits in a particular category can turn this risk into an opportunity for a legitimate company to differentiate itself and its product.
- *Online Sales Channels.* The cyber aspect of counterfeit goods emphasizes sales on social media and e-commerce platforms, as well as company domains. Products sold online often travel through postal services, making the counterfeit goods very difficult to detect before it reaches the consumer. Investment in consumer awareness can help and when detected by a company, law enforcement and the sales platform can become involved.
- *Leveraging Cloud Computing.* Many products such as software, movies, books, and other electronic goods can be easily copied. Advancements in cloud computing has allowed rights owners to conduct real-time verification of licensing rights each time a product is used, preventing multiple copies from being used under the same license. Selling a subscription to an electronic product instead of selling a one-time license also provides an opportunity for greater control over IP rights.
- *Record Copyrights and Trademarks with Customs and Board Protection (CBP).* CBP maintains databases of copyrights and trademarks for use in its inspection process. This information can be helpful in identifying counterfeits in the marketplace. Any collaboration opportunity legitimate companies have with CBP can increase the likelihood of counterfeit products being removed from the marketplace.
- *Watermarking Electronic Products.* This technique can help identify unauthorized product sales and distribution channels.
- *Education of Consumers.* The sales channel is the primary means with which companies interact with consumers. This is an important opportunity for consumers to be educated about purchasing counterfeits and to understand the value behind a brand. Consumers can also be encouraged to report suspicious goods and sellers.



Stage 4: Supply Chain and Distribution

Modern supply chains are more complex and therefore introduce more risk during the product life cycle. Supply chains and distribution networks are also increasingly global in nature, adding different standards and other complicating factors across multiple jurisdictions.

- *Supply Chain Control Risks.* Losing control of proprietary information involving sub-standard knock-offs, and intellectual property violations can pose health and safety concerns for consumers, and associated liability risk.¹ Companies can use the same thinking they have applied to protect against social and environmental risk in supply chains to help protect against intellectual property risk in supply chains.
- *Trusted Supply Chains.* Global supply chains represent opportunities for strengthening governance and developing trusted networks to protect IP. Engaging their supply chains and business networks to drive improvements in labor, health and safety, environment and quality assurance, using supplier codes of conduct, training capacity building, and cross collaboration between the public and private sectors is also crucial in addressing threats to supply chains. This activity turns supply chain risk into opportunity and can become a selling point for a product, brand or company.
- *Utilizing Technology.* Harnessing the power of global supply chains and building upon practical experiences and advancements made in supply chain management firms can leverage current processes and management systems to protect IPR. Technology can now permeate every area of the supply chain. Tracking sensors and other devices embedded in cargo and vehicles provide real-time pictures of assets in the field, while increasingly sophisticated transportation management systems (TMSs) also provide end to end comprehensive transportation management.² In addition, developments in technologies such as Blockchain may provide supply chain assurance capabilities so that companies have better visibility to downstream suppliers and the origin and quality of their components.

Stage 5: Financial Gains and Sustainability

The product life cycle starts and ends with financial matters, from fund raising activity to the process of monetizing company assets, including IP assets and developed products. The ability of a firm to convert IP assets into products, revenue and profit in turn helps that company grow and be competitive and sustainable in the marketplace. Successful innovation drives future innovation and investment capabilities.

- *Licensing and Joint Venture Opportunities.* The product life cycle is primarily about a business developing a product or service and bringing it to market, and it can understandably be the singular focus of the business. But additional opportunities can exist to monetize IP and maximize its value. IP can be a unique asset in that conveying rights to the asset to multiple parties can increase the overall

¹ Insights by Stanford Business, “How Companies Can Protect Themselves Against Intellectual Property Risk in Their Supply Chain”, Hau L. Lee Pamela Passman, February 3, 2014.

² Supply and Demand Change Executive, “Four Trends that Will Shape Supply Chain and Logistics in 2017”, Erik Malin, January 24, 2017.



value—it is not always a ‘zero-sum game.’ This presents an opportunity for IP assets to be out-licensed to other parties, particularly non-competitors in other industries where the IP may have additional uses. Revenue from these licenses can provide needed capital to bring the core product to market.

- *Counterfeiting.* Counterfeiting can directly reduce product sales, but can also have a long-term impact on the sustainability of a legitimate company. Counterfeiters need not adhere to the same regulatory and consumer standards that legitimate companies must and the impact of inferior goods can impact authentic brands and entire product segments. Consumer education and brand loyalty efforts can help. Companies can work with online advertising networks and content owners can pressure websites to remove infringing media. Brand and content owners can work with financial services to shut down accounts receiving payments for infringing goods and media. Companies can leverage voluntary, civil, and regulatory enforcement actions to help with IP protection.
- *Industry Leadership.* Companies can become industry leaders in IP protection and participate in trade groups that can collectively fight IP rights violations in an industry sector.
- *Litigation and IP Defense.* Patents can be costly to maintain because patent infringement must be reported and prosecuted in order to maintain ownership of the patent. There is case law to invalidate a patent if too much time passes before patent infringement is prosecuted by the patent owner.
- *IP Portfolios.* Companies can inventory and value their IP portfolios and look for opportunities to maximize the value of those assets like they would any other corporate asset.
- *Mergers and Acquisitions.* Corporate transactions such as mergers and acquisitions (M&A) are a risk to a company’s IP portfolio. When actual and potential acquirers and partners consider purchasing or partnering with a company they perform due diligence that can include significant access to company business information, including trade secrets. This access can be essential for M&A decision making. An organized M&A process, including the use of NDAs and limited and documented access (data rooms), can prevent IP loss during this period.



Selected Actionable Take-A-Ways for Intellectual Property Protection

- Isolate or compartmentalize different components of proprietary information in-development
- Share only information that would be considered need-to-know
- Maintain strong encryption and multi-factor authentication;
- Uphold security ‘hygiene’ to protect physical infrastructure and computer networks, such as:
 - Require identification and pass codes;
 - Keep networks and building access logs and review suspicious attempts to access;
 - Mandate all visitors and outsiders sign non-disclosure agreements and leave behind any potential recording and storage devices (e.g. tablets, smart phones, wearable technology, and peripheral storage devices like USB sticks);
 - Disable administrator privileges on work devices for all employees;
 - De-activate and disable the ability for unapproved devices to connect to work devices;
 - Limit network connectivity for teleworking employees;
 - Establish strong email filtering and quarantine policies;
 - Maintain frequent and routine encrypted back-ups, and protect such back-up data by maintaining a strong physical control over these servers and by disabling 24-7 network connectivity (i.e., only connect back-up servers during regularly scheduled back-up events);
 - Log all physical and network access, maintain logs on separate devices, and routinely backup logs;
 - Limit or disable the ability of employees to access non-work-related websites;
 - Brief and de-brief all employees who travel frequently on potential security threats while away from the office;
 - Provide employees with “clean” or pre-wiped devices when traveling, and conduct a thorough review of these devices when employees return;
 - Monitor all incoming and outgoing data (including data from internet-connected manufacturing equipment or office-related hardware, such as cloud printers or smart thermostats); and
 - Know what to do and who to contact in the event of an incident;
- Ensure all employees and third-parties who come into contact with proprietary information, or whose work role is essential to the protection of proprietary information, are routinely and frequently informed of and consent to non-disclosure agreements, and are advised of the company’s policies on who owns and retains IP rights.
- Mandate that contractors only use air-gapped devices, or computer networks physically separated and unconnected to the internet.
- Establish drills and security-awareness exercises (e.g. send a dummy phishing email to employees, or make phony phone calls attempting to elicit seemingly innocuous, proprietary information through social engineering) to teach employees about the risks of disclosure and to identify susceptible individuals or departments.
- Apply digital watermarks, fingerprints, and other passive “tells” to highly-sensitive information, or seed digital trade secrets with deliberately missing, false, or misleading information.

