Similarities in Managing Supply Chain Sustainability and Intellectual Property

Barchi Gillai • Sonali V. Rammohan • Hau L. Lee

Knight Management Center
Stanford University
655 Knight Way
Stanford, CA 94305-7298 USA

STANFORD GRADUATE SCHOOL OF BUSINESS

Managing Supply Chain Sustainability and Intellectual Property: Are They More Similar than Different?

Stanford Initiative for the Study of Supply Chain Responsibility (SISSCR)

By Barchi Gillai, Sonali V. Rammohan and Hau Lee

March 2014

Executive Summary

Over the last few years, a growing number of companies have put increased attention on issues related to social and environmental responsibility (SER). As part of this trend, they have been gradually moving away from sole reliance on audits, and instead are focusing more on preventive measures and practices aimed at building supplier capabilities. For the most part, this trend has had a positive impact on companies' ability to drive improvement and reduce the rate of SER-related incidents. Still, other issues, which suffer from similar supply chain lapses, are often managed differently. One such issue is the protection of intellectual property (IP). Despite the growing importance of intangible assets and IP, IP protection is still commonly controlled by the legal department, with most companies failing to take effective action to protect their IP *a priori*. This traditional approach has had limited success, as is evident by the growing magnitude of IP rights violations worldwide. In this paper, we aim to show the value of basing IP protection on an approach similar to the one successfully used to promote social and environmental responsibility, and on embracing a holistic approach to target social, environmental, and ethical responsibility throughout the supply chain. In particular, we discuss the similarities between the underlying causes of SER and IP issues, which suggest that responsible supply chain (RSC) practices found to be linked with reduced SER violations may also be helpful in tackling the issue of IP rights violations. We then show how a RSC framework, consisting of the three main categories of management systems, visibility methods, and response practices, can be applied to IP protection. We also discuss the role of suppliers in respecting and managing third party's IP.

Introduction

In recent years there has been a trend among a growing number of multinational companies (MNCs) to integrate socially and environmentally responsible practices into supply chain operations. Managers have put increased attention on issues related to social and environmental responsibility (SER), and methods to promote responsible practices have become more sophisticated. As part of this trend, MNCs have been gradually moving away from sole reliance on audits, which have proved to be ineffective as a means to ensure compliance. Instead, they are shifting more resources to preventive measures and to building supplier capabilities.

There have been multiple reasons for the growing emphasis on suppliers' full compliance with the laws, rules, regulations, and codes of conduct concerning social and environmental responsibility. An obvious reason is the human and environmental toll of some of the incidents that took place in recent years. Take the tragic collapse in 2013 of Rana Plaza – a commercial building in Bangladesh which housed a number of separate garment factories, where close to 1,200 people were killed. Or consider the oil spill and fire in 2010 at the Deepwater Horizon rig, operated by BP and owned by Transocean, which claimed the lives of

11 people and caused extensive environmental damage. But there are other motivators for firms to be focused on social and environmental incidents occurring in their supply chains. One important reason is that buying companies may be held legally accountable for actions of their suppliers. This point is illustrated by the UN Guiding Principles on Business and Human Rights, which state that among other things, respecting human rights means not "being directly linked by business relationships to an adverse human rights impact.[1]" Incidents such as a factory closure or building collapse may also lead to supply side disruption, negatively impacting supply chain performance and resulting in financial losses. Furthermore, a company's brand image and reputation may be damaged if its suppliers are involved in serious social or environmental incidents. In addition to the risk mitigation and cost containment motivators described here, some firms see a potential for certain RSC practices to enhance brand image and make top-line revenue improvements. For example, several leading companies in the apparel industry are pushing to design more products from environmentally sustainable materials, seeing this as both a sustainability imperative and a business opportunity[2].

For the most part, the growing emphasis on socially and environmentally responsible practices and on supplier capability building seem to be having a positive impact on the ability of MNCs to drive improvement and reduce the rate of SER-related incidents, both internally and at their suppliers' sites. A research study recently conducted by the Stanford Value Chain Innovation Initiative, as part of the Stanford Initiative for the Study of Supply Chain Responsibility (SISSCR), found a positive link between multiple responsible supply chain (RSC) practices and reduced SER violations throughout the supply chain. Some of the practices that were found to be correlated with reduced SER violations include senior management involvement, proactive practices aimed at preventing problems from occurring in the first place, supplier capability building, offering incentives to encourage compliance, and collaboration with suppliers to identify root-causes and take corrective actions whenever a violation is identified[3]. One example of a company taking a collaborative approach is Nike. The company has increasingly linked its sustainability efforts with its innovation efforts, has increased supplier incentives for improving social and environmental conditions, and has focused on systems innovations intended to prevent problems before they arise. This highlights the perceived value Nike sees in using a collaborative and proactive approach[4].

While firms are increasingly managing social responsibility, environmental protection, and ethical issues such as the use of conflict minerals in a more integrated fashion, other issues that suffer from similar supply chain lapses are often managed differently. One such issue is the protection of intellectual property (IP). IP refers to creations of the human mind, which can be commercially used. They may take the form of copyright, patents, trademarks, industrial designs, and geographical indications[5]. In this context, trade secrets

[1] "Guiding Principles on Business and Human Rights," United Nations Global Compact, Last updated: Nov. 2013, http://www.unglobalcompact.org/issues/human_rights/The_UN_SRSG_and_the_UN_Global_Compact.html.
[2] http://www.apparelcoalition.org/higgindex/
[3] Gillai B., Porteous A.H., and Rammohan S.V., "The Relationship Between Responsible Supply Chain Practices and Performance," *Global Supply Chain Management Forum, Stanford University*, Nov. 2013. Available at: http://www.gsb.stanford.edu/scforum/sisscr.
[4] Porteous A.H. and Rammohan S.V., "Integration, Incentives, and Innovation: Nike's Strategy to Improve Social and Environmental Conditions in its Global Supply Chain," *Global Supply Chain Management Forum, Stanford University*, Oct. 2013.
[5] World Intellectual Property Organization (WIPO), "What is Intellectual Property?" *WIPO Publication No. 450(E).* Available at: http://www.wipo.int/about-ip/en/.

are confidential internal business information that provide the basis for competitive advantages and therefore represent a specific form of IP. Trade secrets comprise manufacturing, industrial, or commercial secrets such as business strategies, formulas, technical information and know-how, software and computer programs, production processes, distribution channels, and contact data of suppliers and customers[6]. Due to the characteristic of trade secrets, protecting them can be more difficult than protecting patents or trademarks.

Over the last few decades, intangible assets and IP have become increasingly important in knowledge-based economies[7] and have gained a high relevance for the economic success and value creation of firms[8]. As much as 75% of most organizations' value and revenue sources are in intangible assets, IP and proprietary competitive advantages[9]. Despite that, IP often times does not receive the same kind of attention in the press or Corporate Social Responsibility (CSR) reports. Furthermore, while RSC management is evolving as firms adopt a more holistic approach to target social, environmental, and ethical issues in the supply network, IP protection often times is not considered as part of RSC management, or is only linked with RSC management at a very high level. More commonly, IP protection is controlled by the legal department, with most companies failing to take effective strategic and operational action to protect their IP *a priori*, so as to lower their litigation risk and improve the likelihood of keeping their IP secure. In fact, a survey conducted by the Center for Responsible Enterprise and Trade (CREATe) in collaboration with the Conference Board in 2012 found that for 93% of surveyed companies, the legal department had the primary responsibility for IP protection[10]. This is despite the fact that the same survey highlighted a lack of confidence in this traditional approach and a lack of results. Another hurdle that further limits the effectiveness of IP protection strategies is the tendency of firms to operate in silos, with different organizational units independently determining their own IP strategy.

Given the shortcomings of common IP protection strategies, it is not surprising that IP rights violations and the lack of enforcement thereof are widespread, creating a serious problem for multinational firms. According to a white paper from security firm McAfee, "every company in every conceivable industry with significant size and valuable IP and trade secrets has been compromised (or will be shortly)[11]." The magnitude of the problem has been especially significant in China, where in 2011 the software piracy rate for personal computers was 77%. The commercial value of this unlicensed software is US $8.902 billion[12]. Looking beyond the issue of software piracy to other IP violations, the impacts are much higher. A report

---

[6] WIPO (2013), "What is a Trade Secret?" Available at: http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm.
[7] Organisation for Economic Co-operation and Development (OECD) (2008), "The Economic Impact of Counterfeiting and Piracy," Available at: http://www.keepeek.com/Digital-Asset-Management/oecd/trade/the-economic-impact-of-counterfeiting-and-piracy_9789264045521-en.
[8] Hanel P., "Intellectual Property Rights Business Management Practices: A Survey of the Literature," *Technovation*, 26(8) (2006): pp. 895-931.
[9] www.create.org.
[10] Bayer D.S., Berenbeim R.E., and Walker R., "Safeguarding Intellectual Property and Addressing Corruption in the Global Supply Chain," The Conference Board of Canada, 2012. Available at: http://www.conferenceboard.ca/e-library/abstract.aspx?did=5281.
[11] Alperovitch D., "Revealed: Operation Shady RAT," McAfee, 2011. Available at: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
[12] "Shadow Market: 2011 BSA Global Software Piracy Study," ninth edition, May 2012. Available at: http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

published by the Commission on the Theft of American Intellectual Property estimates the scale of American IP theft reaches over US $300 billion per year[13]. The International Chamber of Commerce estimates that the total global economic and social impacts of counterfeit and pirated products reached about US $775 billion in 2008; this figure was estimated to more than double to US $1.7 trillion by 2015, due in part to a rapid increase in physical counterfeiting and piracy[14]. In addition to financial losses, this development of illicit activities harms the brand and reputation of multinational organizations. Looking beyond impacts of IP theft on individual companies, IP theft is undermining both the means and incentives for entrepreneurs to innovate, therefore slowing the development of new inventions and industries that can further expand the world economy[15].

Given the growing importance of IP and the limited success of existing strategies, the question is then whether multinational firms should modify their approach towards IP protection. Could IP protection be based on an approach similar to the one successfully used to promote social and environmental responsibility? For the next part of this paper, we discuss why we believe that there are enough similarities where greater integration could prove valuable.

It is important to note that, for the sake of simplicity, we reference MNCs as the creators of IP, and suppliers and other trading partners as those that gain access to the MNCs' IP. In practice, MNCs may also have access to the IP of other companies, and suppliers may have their own IP that they need to protect. Therefore, measures should be taken by all companies to protect their own IP as well as IP belonging to third parties.

The Case for a Holistic Approach for Social, Environmental, and Ethical Responsibility

Before exploring similarities between SER and IP issues, it is important to recognize that they differ in multiple ways. SER issues as well as IP rights violations can affect top-line revenue, but the implications of IP violations are likely to be more severe. IP violations can divert demand to cheaper counterfeit alternatives. The introduction of low-quality counterfeits can further diminish demand by damaging the company's reputation and brand image. The impact of IP violations on business profits and share prices can therefore be significant, and is of particular concern given that innovations and corporate-specific IP are expensive to develop and are crucial for maintaining a firm's competitive position. The US $75 billion estimated global annual market worth of counterfeit prescription drugs[16] is a good example of the economic cost of IP violations. SER violations may also damage a company's reputation, but the impact on top-line revenue is likely to be less significant as the public's perception of the company's products is not as likely to be affected. On the flip side, successful development of IP as well as successful SER strategies can enhance

[13] "The IP Commission Report," The Report of the Commission on the Theft of American Intellectual Property, May 2013. Available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
[14] International Chamber of Commerce (ICC), "Impacts of counterfeiting and piracy to reach US$1.7 trillion by 2015," 2011. Available at: http://www.iccwbo.org/News/Articles/2011/Impacts-of-counterfeiting-and-piracy-to-reach-US$1-7-trillion-by-2015/
[15] "The IP Commission Report," May 2013.
[16] Morgan B., "Cracking Down on Counterfeit Drugs," PBS, Aug. 2013. Available at: http://www.pbs.org/wgbh/nova/next/body/uncovering-counterfeit-medicines/.

brand image, leading to higher sales levels. But here again, the impact of IP development on top-line revenue is likely to be more considerable.

At the same time, SER violations are likely to have a greater impact on bottom-line costs. Mattel's 2007 recall of 20 million toys with unacceptable levels of lead paint, which cost the company over US $100 million[17], and Wal-Mart's payment of $82 million for improper disposal of hazardous waste in California and Missouri[18] are just a few examples of the potentially high price tag of SER violations. Supply side disruption due to SER violations can further increase operating costs.

SER and IP issues may also differ in their origin points; while IP infringements may take place upstream and downstream in the supply chain, SER violations tend to occur upstream. Finally, while issues related to IP infringements may vary based on the type of IP in question (e.g., preventing trade secret theft is managed differently than software piracy), the industry a company belongs to may have more of an impact on the SER-related challenges it may be facing (many associations such as the Electronics Industry Consumer Coalition and Sustainable Apparel Coalition are organized to tackle industry-specific issues).

Despite these and other differences between SER and IP issues, several of their underlying causes are very similar. Consider, for example, the lack of visibility into suppliers' practices. Over the last couple of decades, many companies have taken advantage of low material and manufacturing costs in countries such as China, India, Indonesia, and Brazil. But the geographic distance has made it very challenging for the firms to gain visibility into the actual practices of suppliers located in these geographies, limiting their ability to monitor and prevent labor and environmental violations as well as IP leakages.

Another similarity is that suppliers often do not have sufficient incentives to comply with social and environmental requirements or with IP laws. Providing workers with fair wages, limiting the number of overtime hours, and providing proper working conditions can cut from suppliers' profits in the short run; Developing ways to reduce waste and minimize environmental impact may require large upfront investments; And using counterfeit parts or avoid paying software license fees carries with it obvious financial benefits, at least in the short term.

Weak legal frameworks and law enforcement in emerging countries also contribute to the problem. Consider, for example, China, which is faced with severe environmental challenges that must be met in order to prevent the destruction of forests, the extinction of species, the loss of land to desert, and the disappearance of potable water. But China's lack of legal environmental protection results in toxic living conditions and leaves environmental advocates without tools to protect the environment and themselves[19]. As for IP protection, while China has acceded to the major international conventions on protection of IP rights and has created a comprehensive legal framework to protect both local and foreign IP, these laws have rarely been enforced in the past due, at least in part, to the short-term economic benefits of piracy and

[17] Lefevre C., et al., "Value of Sustainable Procurement Practices. A quantitative analysis of value drivers associated with Sustainable Procurement Practices," PwC and EcoVadis in collaboration with the INSEAD Social Innovation Centre, 2010.
[18] Clifford, S., "Wal-Mart Is Fined $82 Million Over Mishandling of Hazardous Wastes," *The New York Times*, May 29th 2013.
[19] Goelz, D.J., "China's Environmental Problems: Is a Specialized Court the Solution?," *Pacific Rim Law & Policy Journal*, Vol. 18 No. 1, 2009. Available at: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/522/18PacRimLPolyJ155.pdf

misuse of IP[20]. Cultural differences also contribute to the problem, as the notion of IP protection as an individual rather than a state right was relatively foreign in ancient Chinese society and has been recognized by China for only about thirty years[21]. Consequently, China is now the world's single largest producer of pirated goods, with an extensive and sophisticated network of infringers who pirate products of virtually every industry[22]. It is important to note that while beneficial to China in the short run, piracy has had unsettling long-term effects on the Chinese domestic economy, as well as on China's goal of shifting the focus of its economy from low-productivity manufacturing to a balanced economy focused more on scientific innovation[23]. Consequently, China has started taking more steps to strengthen IP protection, including the launch in March 2013 of the Norms for Enterprise IP Management, as part of China's Promotion Plan for the Implementation of the National IP Strategy[24]. But even with this new focus, it is likely to be awhile before adequate levels of IP enforcement can be achieved in China.

Another similarity between the two areas is that for both IP management and SER practices, employees play an important role in implementing corporate strategy. In the context of IP thefts, employees are often the leakage points of confidential information[25]. With SER, employee awareness and understanding of corporate values are the basis for the successful implementation of SER aspects in daily working routines[26].

Similarities between several underlying causes of social, environmental, and IP issues suggest that RSC practices linked with reduced SER violations may be helpful in tackling IP infringements.

The similarities between some of the underlying causes of social, environmental, and IP issues along the supply chain suggest that several RSC practices linked with reduced SER violations may also be helpful in tackling IP infringements. This line of thought is supported by feedback collected in 2013 from participants of CREATe's IP Protection program. 100% of the companies that completed CREATe's independent evaluation considered a management systems approach to IP protection to be very effective, and believed it would enable them to better protect their IP and that of their customers.

"Sense and Response" RSC Framework

Exhibit 1 displays a proposed "Sense and Response" Responsible Supply Chain Framework, which was constructed based on CREATe's Leading Practices management system, inputs from members of SISSCR,

[20] http://en.wikipedia.org/wiki/Intellectual_property_in_China
[21] Kassner G., "China's IP Reform: State Interests Align with Intellectual Property Protection (Again)," *JOLT Digest*, April 2012. Available at: http://jolt.law.harvard.edu/digest/patent/chinas-ip-reform-state-interests-align-with-intellectual-property-protection-again
[22] Kassner G., "China's IP Reform."
[23] Kassner G., "China's IP Reform."
[24] "China: IP Management Standard," *CREATe Views Blog*, January 2014. Available at: http://www.create.org/views-blog/china-ip-management-standard.
[25] Reid D. and MacKinnon S., "Win the China IP War and Gain Globally," *Thunderbird International Business Review*, 52(6) (2010): pp. 475-489.
[26] Inyang et al., "CSR-HRM Nexus: Defining the Role Engagement of the Human Resources Professionals," *International Journal of Business and Social Science*, 2(5) (2011), pp. 118-126.

existing literature, and CSR reports. It includes three main categories: Management Systems, Visibility Methods, and Response Practices. Following a brief description of the framework, we discuss how it can be applied to IP protection.

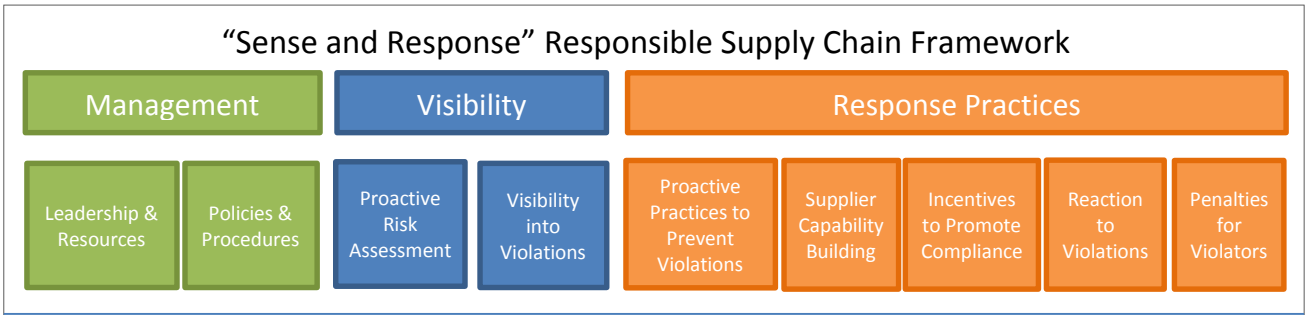

Exhibit 1

Management Systems: The management system lays the foundation for responsible practices across the supply chain, and is based on buy-in and leadership from top executives; dedication of sufficient resources; establishment of uniform policies and procedures across the supply base; and collaboration with peer companies on development of responsible practices.

Visibility Methods: Visibility can be defined as the increase of available data that can shed light on issues in the supply chain, and can be analyzed to make recommendations and determine strategies to improve and strengthen the supply chain. Visibility methods should help identify existing violations and other issues in the supply chain, as well as potential problems that may develop into serious issues in the future.

Response Practices: Response practices are actions taken in response to identified violations or preventative measures that help avert potential issues from developing into major problems. Some of the actions taken in response to identified violations may include root cause analysis, development of corrective action plans and assisting suppliers in the implementation of such plans, as well as monetary fines and other penalties to suppliers with severe or ongoing code of conduct violations. Preventive measures may include incentives to suppliers to encourage compliance, supplier capability building through training and diffusion of best practices, and proactive practices such as product and process redesign, improved information sharing, and providing suppliers with resources to allow them to address root causes independently.

The research conducted recently by Stanford, as part of SISSCR, identified a positive link between many of these practices and reduced SER violations. In particular, our research suggests that senior management involvement, supplier collaboration and capability building, supplier incentives and more proactive practices aimed at preventing problems from occurring in the first place are associated with SER performance improvement and lower operating costs. We next explore how the same Sense and Respond Responsible Supply Chain framework can be used to improve IP protection capabilities.

IP Protection in the Context of a RSC Framework

IP issues can be divided into two main categories: criminal activity, such as theft of trade secrets for commercial advantage or trafficking in counterfeit goods, and the misuse of IP by legitimate businesses due to poor procedures, low awareness, and loose controls. Existing management literature provides guidelines, recommendations, and frameworks on how firms can address both types of IP issues within their

companies and their supply chains. Naturally, the recommended practices are tailored to the specific challenges associated with IP protection. Still, at a higher level, many of them fall within the Responsible Supply Chain Framework. The following are examples of practices that can reduce the risk of IP infringement, which relate to the three broad areas of management systems, visibility methods, and response practices[27].

Management Systems: Some practices found to be linked with reduced SER violations include senior management involvement, dedication of sufficient resources, organization of SER management as a cross-divisional function, and participation in industry working groups (e.g., the Electronics Industry Citizenship Coalition and the Sustainable Apparel Coalition). Similarly, management systems can be put in place to protect an organization's IP. A mature and well-implemented management system can supplement the work currently done by the legal department in many organizations, weave IP protection into the culture of the company and its business operations, help to prevent IP infringement inside the company and its supply chain, and eliminate unintentional lapses in IP protection. We highlight four aspects of management systems that can strengthen IP protection below.

- **Leadership:** IP protection is difficult to coordinate because it is integrated along the entire value chain. Various corporate departments can be the source for leaks. Even though integrating management across different corporate departments is essential for proper IP protection, large firms often lack an overall IP protection strategy[28]. IP management and protection might therefore be more effective in a centralized department, with head office support, and a cross-divisional function, which aims to preserve confidential information within the firm and throughout the value chain. The involvement of senior and top management as well as the R&D department is likely to further improve the protection of valuable IP[29], as top management involvement ensures awareness for IP issues and the enforcement of IP protection measures.

Siemens has established a central Corporate IP department, which coordinates the company's IP policies, IP protection measures, and IP strategies.

- **Policy:** Rather than let different divisions and business units be in complete charge of IP protection policies related to their own operations, the International Chamber of Commerce (ICC) recommends establishing of a corporate-wide IP policy, which would constitute the basis from which to develop and implement IP strategies, procedures, and practices for the protection of corporate confidential information[30]. The IP policy should also provide a framework for discussions with suppliers and other business partners regarding their own obligations with regards to IP protection. To ensure that the IP policy is workable and continues to address the evolving challenges faced by the company, it should be reviewed and refined periodically. Siemens is one example of a company that has established a central Corporate Intellectual Property department, which coordinates the company's IP policies, IP

[27] This section is based on Schneider, A.M, "Integration of IP Protection in the SER Framework," 2014.
[28] Reid, D. and MacKinnon, S., "Win the China IP War."
[29] Al-Aali, A.Y. and Teece, D.J., "Towards the Strategic Management of Intellectual Property: Retrospective and Prospective," *California Management Review*, 55(4) (2013), pp. 15-30.
[30] ICC, "Intellectual Property - Guidelines for Business," 2011. Available at: http://www.iccwbo.org/advocacy-codes-and-rules/bascap/value-of-ip/ip-guidelines-for-business.

protection measures, and IP strategies, while still allowing individual divisions to align their IP strategy to their business plans, environmental factors, as well as the institutional framework in the respective region of activity[31]. One source companies may use in developing their IP protection policies is the IP Model Policies developed by CREATe, which provide a framework that can be adapted to the specific requirements and situation of each organization[32].

- **Evaluation and Assessment:** Naturally, not all IP impacts a company's competitiveness in the same way. In order to improve resource allocation and increase the overall effectiveness of IP strategies, it is recommended for companies to classify their at-risk IP into categories – e.g. high value, medium value, and low value – and to develop different policies for the protection of IP in each category: high value IP would require the most robust, and likely the most costly protection mechanisms, while low value IP would likely only need a basic protection plan[33].

- **Collaboration with Peer Companies and Associations:** Collaboration between multinational organizations may help expose the sources of IP leakages, and further the development of methods to resolve IP issues in developing nations[34]. A number of related associations already exist, such as the Open Group Trusted Technology Forum (www.opengroup.org), which has developed an open standard and an accreditation program for technology providers in order to support multinational organizations in improving security along the supply chain and finding appropriate business partners. CREATe (www.create.org), The International Electronics Manufacturing Initiative (www.inemi.org), The Conference Board (www.conference-board.org), and The Common Criteria (www.commoncriteriaportal.org) also aim to enhance IP protection.

Visibility Methods: While higher visibility should not by itself be relied on to increase compliance, it is an important part of the process, as companies must first gain an understanding of potential risks and existing issues before they can determine how best to address them. The Stanford study found that practices aimed at increasing visibility such as risk assessments and audits conducted at set intervals and based on multiple sources of information, construction of corrective action plans, and clear communication of these plans were positively linked with reduced SER violations. These monitoring and visibility systems were found to be especially valuable when extended beyond internal operations to external business partners.

Through visibility methods, companies can gain an understanding of potential risks and existing issues.

Similarly, experts recommend that MNCs conduct risk assessments to identify IP protection risks. These may include risk assessments of new products, services, and business opportunities, as well as due diligence and risk assessment on all relevant supply chain members. Furthermore, it is recommended that MNCs establish and operate a system to routinely monitor their performance and the performance of their supply

[31] Ma A., "SIEMENS: customized and regional IP strategies," *China IP*, 23, April, 2008. Available at: http://www.chinaipmagazine.com/en/journal-show.asp?id=285.
[32] CREATe Model IP Protection Policies, available at: http://www.create.org/tools-training/tools/model-policies-0.
[33] Reid and MacKinnon, "Win the China IP War."
[34] Reid and MacKinnon, "Win the China IP War."

chain members in meeting the company's relevant IP policies[35]. A growing number of companies are monitoring IP protection as part of holistic supplier assessments, which also examine other risk factors such as quality, financial stability, labor and environmental protection.

MNCs may rely on supplier firms to control and communicate their IP policies and IP protection procedures in line with the requirements of their customers, or they may monitor suppliers through audits. MNCs should be cautious though with regards to audit results, as audit fraud can be widespread in countries such as China[36]. An indirect way to detect IP infringement is through the review of suppliers' patent and trademark portfolio, and the way it changes over time[37]. The frequency of audits and other data collection should be based on the risk level for IP infringement and theft by the respective supplier.

Response Practices: Companies use information gained through visibility methods to take action in response to violations that have already occurred, or to mitigate risks and prevent future problems. The Stanford research found that proactive measures to prevent violations, such as product and process redesign, supplier capability building, and providing incentives to encourage compliance, were among the most strongly correlated with reduced SER violations. Measures taken in response to identified issues, including root cause analysis and assisting suppliers in the implementation of corrective actions, were also found to be linked with reduced SER violations. Similar strategies can be used by multinationals to reduce the risk of IP infringements. We list key examples below.

- **Proactive Practices to Prevent IP Leakages:**

  Access Limitation: It is critical for companies to maintain physical and electronic security to protect trade secrets and other confidential and propriety information. Trade secrets and other propriety information should be made available to employees and third parties on a need-to-know basis, and subject to company procedures and confidentiality agreements[38]. Multiple technological innovations can also be used by companies to safeguard their IP, examples of which include encryption of confidential information; restrictions on electronic documents so that they exist only for a limited amount of time, can only be accessed with a special code, and are restricted from being saved, forwarded, or printed[39]; and more. Similar mechanisms can also be integrated into products, such as a cryptosystem integrated into Microsoft's Xbox™ [40].

  IP protection mechanisms can be integrated into products, such a cryptosystem integrated into Microsoft's Xbox.

[35] CREATe Model IP Protection Policies.
[36] "A Look at How Some Chinese Factories Lie to Pass Audits," *China Labor Watch*, April 2012. Available at: https://www.chinalaborwatch.org/news/new-413.html.
[37] Firth G., "IP Protection Best Practice Tips, The best offense is a good defense—and vice versa," *The China Business Review*, 33(1) (2006): pp. 18-25.
[38] CREATe Model IP Protection Policies.
[39] Mattioli D., "In China, Western Firms Keep Secrets Close," *The Wall Street Journal*, Aug. 30, 2010. Available at: http://online.wsj.com/article/SB10001424052748704913704575453612099883050.html.
[40] Huang A., "Keeping Secrets in Hardware: The Microsoft Xbox™ Case Study," Kaliski B.S. Jr. et al. (Eds.): CHES 2002, LNCS 2523, pp. 213-227, 2003.

Modular Structure: One successful strategy for protecting IP is through system decomposition of the R&D process[41]. High-value core R&D processes take place in the home country of the multinational organization or other developed countries with a powerful IP protection framework, while non-core and well protectable R&D activities are realized in emerging countries in order to benefit from low costs and local talent pools.

The decomposition may also take place at the production level. For instance, Cree Inc., a Durham, U.S. based manufacturer of light-emitting diode (LED) lights and components, manufactures LED wafers in the U.S., then has the components transported to China where they are integrated into the final product in the Cree-owned production plant[42]. However, such an approach may sometimes be too time-consuming and expensive to be practical[43].

Cree Inc. manufactures LED wafers in the U.S., and then transports them to China for integration into the final product.

Former Sony Ericsson has followed another strategy. The company has restricted its outsourcing to the production of aging products only. This way, new and highly valuable IP and product ideas are protected in countries with strong enforcement[44].

Employee Hiring and Training: Employees in multinational organizations as well as supplier firms are among the most vulnerable IP leakage points. Therefore, during the recruiting process attention should be paid to the related risks, and new employees should be required to sign non-compete and non-disclosure agreements[45]. Furthermore, employees and suppliers that operate with confidential business information and high-value IP should be trained periodically so they understand the importance of IP for the company, the need to protect the company's and third party's IP, and the requirements from each employee.

- **Supplier Selection and Capability Building:**

Supplier Selection and Evaluation: Generally, supplier selection should be an integral part of IP protection, and evaluation of the supplier's IP protection program maturity should be a critical component of the selection process. Characteristics such as technological capabilities and level of integrity should be taken into consideration when determining whether to engage with a new supplier and what IP may be shared with them. Suppliers with their own technological capabilities and low integrity pose a higher risk and are more susceptible to IP infringement[46]. In these cases, further due

[41] Quan X. and Chesbrough H., "Hierarchical Segmentation of R&D Process and Intellectual Property Protection: Evidence From Multinational R&D Laboratories in China," *IEEE Transactions on Engineering Management*, 57(1) (2010), pp. 9-21.
[42] Mattioli, "In China, Western Firms Keep Secrets Close."
[43] Deng X. et al., "Product decomposition using design structure matrix for intellectual property protection in supply chain outsourcing," *Computers in Industry*, 63(6) (2012), pp. 632-641.
[44] Arruñada B. and Vázquez X.H., "When your contract manufacturer becomes your competitor," *Harvard Business Review*, 84(9) (2006), pp. 135-144.
[45] Reid and MacKinnon, "Win the China IP War."
[46] Wu F. et al., "Supplier selection for outsourcing from the perspective of protecting crucial product knowledge," *International Journal of Production Research*, 51(5) (2013), pp. 1508-1519.

diligence and risk assessment of suppliers are suggested before sharing valuable IP[47]. IP theft may take place at multiple nodes along the value chain[48], so distributors should also be assessed in addition to suppliers.

Relationship Building: After selecting suppliers, the type of relationship developed may impact the supplier's access to sensitive and high-value IP, as well as their motivation to avoid IP violations. Relationships with suppliers can range from a one-time agreement to long-lasting strategic alliance. The type of relationship developed should be based on the complexity and novelty of the products or components supplied by that supplier, and the type of information that must be shared with them[49].

Capability Building: Sometimes, suppliers and other business partners may need guidance and assistance in determining the best way to safeguard IP. MNCs may help their suppliers to develop their IP protection capabilities by providing training, working with suppliers to identify risk factors, sharing best practices, and more. Our research identified capability building as being linked with reduced SER violations. We believe it is likely that it can also strengthen suppliers' IP protection capabilities.

Vertical Expansion / Joint Venture: Typically, MNCs' sourcing alternatives can be divided into three general categories: 1) captive sourcing (low IP risk and high costs), 2) unaffiliated supplier (high risk and high flexibility), and 3) joint venture (medium risk and medium costs). One reason for companies to set up majority-owned joint ventures (JVs) in emerging nations is so that they can better protect their corporate IP by being in charge of the hiring process. Terex Corp is one example of a company that prefers Chinese joint ventures with majority ownership, to oversee IP handling within the company[50]. At the same time, while JVs provide a less expensive way of sourcing compared to captive sourcing, companies should be careful when participating in such a form of collaboration, as JVs have been often used in the past by Chinese companies to get access to and steal confidential corporate information and MNCs' know-how[51].

- **Incentives:**

The prospect of a long-term relationship with the buying company is one way to motivate a supplier to take action to minimize IP theft.

Providing incentives to a supplier, such as investment in training and education and public recognition, were found to be linked with reduced SER violations. They may also be valuable in increasing IP compliance, as IP infringements may carry with them financial benefits to the violating party, and taking steps to identify leakage points of confidential information requires financial resources. At present, however, multinationals typically do not offer their suppliers any incentives to elicit compliance with IP rules and regulations. It is recommended for MNCs to re-evaluate this practice, and consider offering their suppliers incentives tied to IP protection. The prospect of a long-term relationship with the buying company is one way to motivate the supplier to take action to minimize IP theft. Some

[47] CREATe, "Trade Secret Theft - Managing The Growing Threat in Supply Chains," 2012. Available at: http://www.create.org/news-resources/resources/trade-secret-theft-supply-chains.
[48] Firth, "IP Protection Best Practice Tips."
[49] Arruñada and Vázquez, "When your contract manufacturer becomes your competitor."
[50] Mattioli, "In China, Western Firms Keep Secrets Close."
[51] CREATe, "Trade Secret Theft."

companies, such as Microsoft, incorporate IP protection into their supplier scorecard. If future business engagement and financial relationships depend on the supplier's score, the company may be more prone to protecting IP as well.

- **Reaction to Violations:**

  When a violation of IP rights is identified, one course of action is to take legal measures to penalize the violating party. But in addition, it is recommended for the buying company to investigate how the IP leakage was made possible, build a corrective action plan, and follow up to verify its full implementation. In case the IP infringement takes place at a supplier site, it can be valuable to involve the supplier in this process. Sometimes MNCs may prefer to forego the legal route all together, and focus instead solely on corrective action. This was the case with a global consumer electronics company, which discovered in 2010 that its largest licensed distributor was selling knockoffs of its product to retailers, mixed in with the real product. Even though legal action was warranted, it was not an attractive option due to multiple reasons. Instead, the company implemented new procedures to prevent counterfeits from entering the supply chain and rolled out new controls, resulting in complete elimination of the counterfeit problem within a year, while maintaining good business relations with the distributor[52].

- **Penalties:**

  MNCs may try to enforce their IP rights through legal measures, which in some cases may lead to high fines and prison sentences[53]. However, legal frameworks and laws for IP rights vary around the world, and law enforcement is often weak, especially in emerging nations[54]. This may limit the effectiveness of lawsuits as an instrument for deterring IP violations. A similar observation was made in our SER-related research, where penalties for SER violations were found to be ineffective for the most part.

The Role of Suppliers

So far the discussion has focused on practices that MNCs can implement to help protect their own IP across the supply chain. But suppliers, who have access to their customers' confidential information, and may also be using proprietary products such as software solutions for their day-to-day operations, also have a role in protecting other companies' IP.

There are a number of reasons for suppliers to take such action, despite the associated costs. One reason is that being able to demonstrate ethical behavior can provide a competitive edge to suppliers who are looking to differentiate themselves, as a growing number of companies are looking to deal with ethical, stable, and responsible suppliers.

When considering software usage, an additional key motivator should be the negative impact that pirated software may have on effective business operations, competitive advantage, and information security. The

[52] Moss, C., "Addressing the Challenge of IP Theft," CREATe.org, Dec. 2013.
[53] Ong, R., "Trade Secret Enforcement in China: Options and Obstacles," *China Business Review*, January-March 2013, pp. 48-51.
[54] Quan and Chesbrough, "Hierarchical Segmentation of R&D Process."

detrimental effects of pirated software are evident through findings of a 2011 Harrison Group study. According to this study, nearly one in four (24%) pirated operating systems observed either became infected at installation or independently downloaded and installed malicious software upon connection to the internet. Furthermore, the study found that computers installed with genuine Microsoft products were more energy efficient, and provided superior performance in the form of faster boot times, faster print times, and faster loading times[55].

Beyond direct benefits to suppliers, ensuring clean IT at the supplier level is crucial for the entire supply chain. According to Symantec's 2013 Internet Security Threat Report[56], 2012 saw a 42% increase in targeted cyber-attacks compared to a year earlier. Fifty percent of all the targeted attacks were aimed at businesses with fewer than 2,500 employees; 31% of all attacks targeted small businesses with less than 250 employees. While it can be argued that the rewards of attacking a small business are less than what can be gained from a large enterprise, this is more than compensated by the fact that many small companies are typically less careful in their cyber-defenses. Furthermore, many of the cyber attackers may not necessarily be only after information retained by these small businesses. Rather, attackers deterred by a large company's defenses often choose to breach the lesser defenses of a small business that has a business relationship with the attacker's ultimate target, using the smaller company to leap frog into the larger one.

Beyond direct benefits to suppliers, ensuring clean IT at the supplier level is crucial for the entire supply chain.

Therefore, it is essential to raise awareness of the risks of poor IT system management and encourage suppliers to be proactive in ensuring their IT environments are more secure and compliant. The benefits of doing this can accrue to suppliers, buyers and economies globally.

Suppliers can use multiple practices out of the RSC framework presented in Exhibit 1 to safeguard IP. Such practices may include the establishment of a management system that ensures business is conducted in compliance with IP-related laws, that third party's IP is not infringed knowingly, and that no counterfeit or other infringed goods are being used in running its business. Suppliers should also conduct risk assessments and use audits or other methods to identify risks and existing violations. Finally, suppliers may adopt a variety of practices to increase compliance, including employee screening and routine training, limiting access to confidential information, and process redesign to minimize the danger of IP leakages.

Data collected by CREATe in 2013 from a select group of 37 suppliers show mixed results with regards to the maturity of their IP protection practices. While there is a growing awareness among company executives to the critical role of proper management of IP protection, most companies are not taking enough action. For example, while most companies have some policies and procedures in place, they are often incomplete and tend to focus primarily on IT and physical security. Procedures are also often lagging behind policies, making effective implementation difficult. Many companies have good security measures in place to protect

[55] Braskamp C. and Soffronoff J., "Genuine Microsoft Products vs. Pirated Counterparts," Harrison Group, Aug. 2011. Available at: http://www.microsoft.com/en-us/news/presskits/antipiracy/docs/genuinemsproducts.pdf.
[56] Available at: http://www.symantec.com/security_response/publications/threatreport.jsp?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Apr_worldwide_ISTR18.

IP in either physical or electronic format. But risk assessments and monitoring are often times limited, and tend to be reactive[57].

There are a number of external resources that suppliers may use to help them assess and enhance their IP protection capabilities, such as CREATe's Leading Practices for IP Protection program, which offers an evaluation of the company's current practices, as well as a roadmap and multiple resources to help companies benchmark and improve their practices for safeguarding IP. Another resource is Verafirm[58], an online portal created by BSA | The Software Alliance, which helps organizations of all sizes to understand and manage their software assets effectively.

Verafirm is especially helpful for smaller suppliers, who may not have sufficient resources to develop their own software asset management (SAM) solutions to ensure compliance. Larger companies may choose instead to develop their own proprietary SAM solutions, and tailor them to their specific needs and challenges. One such example is Flextronics. In an effort to ensure software compliance, which was one of their biggest challenges, the company created a global software system that allows them to constantly monitor and reconcile their software usage, in an efficient and cost-effective way[59].

Conclusion

The growing importance of intangible assets and IP, and the shortcomings of existing IP protection strategies, call for a revision to these strategies. Given the similarities between many of the underlying issues that lead to SER violations and IP infringements, we believe that companies will benefit from aligning their IP protection strategies with those strategies that are associated with improved SER performance. By using a more holistic approach to tackle social, environmental, and ethical issues throughout the supply chain, it is possible to improve performance. In particular, companies are likely to benefit from establishing management systems that lay the foundation for respecting and protecting IP, and from focusing on practices such as risk assessments, supplier capability building, and the implementation of preventive measures to eliminate risk factors. Such proactive practices aim to drive continual improvement and prevent IP infringements, rather than today's more reactive approach to protecting IP.

The authors would like thank Anne Kelley of Microsoft Corporation and Craig Moss of CREATe for their valuable comments and insights, and also thank Craig Moss for sharing data from CREATe's Leading Practices pilot. We would like to acknowledge Dr. Anna-Maria Schneider from Humboldt University of Berlin for her research, which provided the basis for our discussion on IP protection strategies in the context of a responsible supply chain framework. We thank Angharad Porteous for her insights in the early stages of developing this paper. Finally, we thank members of the Stanford Initiative for the Study of Supply Chain Responsibility for their support.

[57] CREATe.org, "Leading Practices: Pilot Program Results Report," Feb. 2014. Available at: http://www.create.org/create-leading-practices-pilot.
[58] Available at www.verafirm.org.
[59] Based on a video at www.verafirm.org