

Trade Secret Theft

MANAGING THE GROWING THREAT
IN SUPPLY CHAINS

CREATE.org
Center for Responsible Enterprise And Trade

TABLE OF CONTENTS

pg. 1	An Introduction
2	Executive Summary
4	Part 1 Trade Secret Misappropriation is a Large and Growing Problem.
10	Part 2 The Risks of Trade Secret Theft are Magnified when Companies Extend their Supply Chain Overseas.
16	Part 3 The Weak Rule of Law in Many Countries Makes it all but Impossible for Multinational Corporations to Address Trade Secret Theft After the Fact.
20	Part 4 Proactive Measures Must be Implemented Across Organizations to Prevent Rampant Trade Secret Theft.
26	Endnotes

Contributors

This report was developed by the Center for Responsible Enterprise and Trade (CREATE.org) with thanks for the contributions of **Josephine Liu** and **Laurie Self**.

AN INTRODUCTION

Over the past 30 years, international trade has increased more than sevenfold and now represents a third of all global economic activity. This transformation means that millions of people have entered the economic mainstream for the first time, raising income levels, creating new jobs, and contributing to better access to education and healthcare. If the expansion of prosperity in our current era is to continue into the future, we have no choice but to reinforce and strengthen the conditions that make such economic growth possible.

A critical component for strengthening business conditions globally is addressing the prevalence of trade secret theft—an issue that costs multinational companies (MNCs) billions of dollars each year.

Trade secret misappropriation is a threat that raises barriers for people, economies, and businesses that compete fairly. It harms efforts to create jobs and stimulate growth. It also provokes counterproductive behavior that—if left unchecked—will have severe and lasting consequences on the global economy.

Because many of the global markets where MNCs now operate lack an enforceable framework of laws and regulations, the onus of protecting trade secrets often falls on individual companies. As such, MNCs would benefit from playing a more deliberate and proactive role in protecting their trade secrets across their global supplier networks.

The Center for Responsible Enterprise And Trade (CREATe.org) produced this white paper to spark a public dialogue about how far-reaching and deeply challenging the trade secret issue is for MNCs, and to offer companies practical guidance on securing their supply chains and mitigating the significant risks and costs associated with trade secret theft. We hope you find this information insightful, and the proactive measures useful.

For more information or to learn how to get involved in our efforts, we invite you to visit us at www.CREATe.org.



Pamela S. Passman

President and Chief Executive Officer
Center for Responsible Enterprise and Trade (CREATe.org)

The background of the entire page is a low-angle, upward-looking photograph of a modern glass skyscraper. The building's facade is composed of a grid of dark metal frames and large glass panels. The perspective creates a sense of height and scale, with lines converging towards the top of the frame. The entire image is overlaid with a solid blue color, which is lighter in the upper left corner where the text is located and gradually darkens towards the bottom and right edges.

EXECUTIVE SUMMARY

Trade secret theft costs industry billions of dollars each year, and no company is immune. Any company with valuable commercial information, processes, or intellectual property — in other words, virtually every company in the world — is vulnerable to trade secret misappropriation.

Several economic trends have escalated the risk and prevalence of trade secret theft, including the globalization of trade and interconnected supply chains, the growing importance of innovation and information technology to competitiveness, and the rise of overseas markets as a critical source of production and economic opportunity.

In countries with a weak rule of law, trade secret theft is so pervasive and so clearly a part of a strategy in certain intellectual property-intensive industries that supply chains in operation in those countries inevitably create vulnerabilities and access points for theft of trade secrets. Companies have suffered crippling financial losses, been forced to eliminate jobs, and scaled back or even terminated their operations because of trade secret theft in countries where there is weak rule of law.

Nevertheless, for many companies, global sourcing is an economic imperative and a means of expanding their business in high-growth markets. The question then is how best to take full advantage of the benefits of a global economy without jeopardizing business-critical trade secrets and other valuable intellectual property (IP). To mitigate the significant risks and costs of trade secret theft, companies should proactively implement a range of best practices to secure their supply chains. Such measures should elevate the importance of trade secret protection in supplier relationships and help create much-needed disincentives for theft.

As described in part 4 of this paper, companies should:



1. Conduct a strategic assessment of the company's trade secrets, a process which should incorporate the company's trade secret policy, supplier code of conduct, an evaluation of which trade secrets can be transferred, and careful consideration of the most appropriate operational structures.



2. Undertake appropriate pre-contractual due diligence, including a thorough assessment of any potential supplier, evaluation of other IP-related issues, analysis of the supplier's employment and nondisclosure agreements, and investigation of the supplier's subcontractors.



3. Employ strong contractual protections to safeguard the company's trade secrets both during the business relationship and afterward, and consider contractual provisions specifically relating to the supplier's employees and subcontractors.



4. Utilize appropriate operational and security measures to ensure that the correct personnel, physical security measures, and technical safeguards are in place to protect the company's trade secrets. Systematic engagement with the supplier can help bolster the effectiveness of these measures.



5. Take appropriate action after the business relationship has ended, to ensure that departing employees and former business partners honor their continuing obligation not to disclose trade secrets.

Taken together, these measures can help ensure that companies reap the rewards of their investment in research, innovation, and intellectual property.



1 •

TRADE SECRET
MISAPPROPRIATION
IS A LARGE AND
GROWING PROBLEM.

Companies often pour millions of dollars and years of research into developing proprietary technologies, manufacturing processes, and other confidential information — only to find themselves competing against rivals who have stolen their market-leading innovations and who are now churning out the same products at a fraction of the cost.

Trade secret theft can affect every company and every industry sector, and the rise of cybertheft has only made the problem worse. Criminals, competitors, and governments are deliberately targeting advanced technologies and information assets, a fact which should concern any organization with a substantial supply chain.

Everyone is vulnerable, and the risks are significant.

According to a recent white paper from security firm McAfee, “every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly).”¹ In fact, McAfee’s vice president of threat research went so far as to say, “I divide the entire set of Fortune Global 2,000 firms into two categories: those that *know they’ve been compromised* and those that *don’t yet know*.”²

Considering that “as much as 75 percent of most organizations’ value and sources of revenue (or wealth) creation are in intangible assets, intellectual property, and proprietary competitive advantages,”³ it is no surprise that information assets of all types are being targeted. A study of trade secret cases litigated in U.S. federal district courts found that a diverse spectrum of trade secrets were at risk: formulas; technical information and know-how; software or computer programs; customer lists; internal business information such as marketing, finance, or strategy information; external business information such as information about suppliers, competitors, or other industry participants; trade secrets involving a combination of elements that are individually in the public domain; and negative trade secrets such as knowledge of past mistakes or

results of failed experiments.⁴ Although most of the existing data and research has focused on U.S. companies suffering from trade secret theft, similar research conducted in Europe or elsewhere would undoubtedly show a comparable impact.

Billions of dollars are lost each year due to economic espionage,⁵ and even one incident can significantly affect a company’s competitiveness. For example, after a former Ford Motor Co. engineer copied 4,000 Ford documents onto an external hard drive and went to work for a competitor, Ford estimated that it suffered more than \$50 million in losses.⁶ A similar case occurred at Valspar Corporation, where an employee unlawfully downloaded proprietary paint formulas with the intent of taking them to a new job. The formulas were valued at \$20 million — about one-eighth of Valspar’s reported profits in the year the employee was arrested.⁷ On average, companies in the product development and manufacturing industry lost \$4.6 million worth of intellectual property in 2008.⁸

Moreover, when companies experience a loss of this sort, it can harm their business in many different ways. When asked about the business impact from their single most significant incident, U.S. companies reported that they had suffered or anticipated a loss of competitive advantage in a single or multiple products or services; a loss of core business technologies or processes; a loss of company reputation, image, and/or goodwill; reduced projected/anticipated returns or profitability; increased vulnerability to terrorist threats; and a loss of information or prototypes that could facilitate product counterfeiting.⁹ A data breach can also delay or block strategic business initiatives, such as a corporate acquisition or a new product rollout.¹⁰

Trade secret theft is on the rise, due in part to increased cybercrime.

As Figure 1 illustrates, the number of trade secret theft cases in U.S. federal courts doubled between 1988 and 1995, and doubled again between 1995 and 2004.¹¹ The number of trade secret cases in Europe appears to be increasing rapidly as well.¹²

One of the factors contributing to the exponential rise in trade secret misappropriation is the increasing use of technology—both by the companies who own valuable corporate information and the malicious actors who want to steal that information. The storage of data overseas “has made intellectual capital theft more prevalent and prosecution much more difficult.”¹³ The growing trend toward perpetual connectivity to internal computer networks and the Internet also makes it easier than ever to access and steal corporate data from anywhere, at any time. Last year, Cisco predicted that there would be more than 15 billion network-connected devices by 2015.¹⁴ And the trend toward globalized supply chains for IT products creates “more opportunities for malicious actors to compromise the integrity and security of these devices.”¹⁵

Technological developments have also emboldened cyberthieves, who are discovering new reasons and ways to steal corporate data. In the words of a U.S. Treasury Department official: “Before, criminals used to steal money to become rich, but now they have realized that they can be rich by stealing corporate information.”¹⁶ McAfee calls corporate intellectual capital “the new currency of cybercrime.”¹⁷ For example, “the ‘Night Dragon’ attacks on oil and gas companies around the world ... over a period of several months silently and insidiously exfiltrated gigabytes of highly sensitive internal information including proprietary information about field operations, project financing and bidding documents.”¹⁸ In a survey of global firms, 39 percent of respondents identified “attacks from data thieves” as a threat to their corporate information.¹⁹

It is not just outside attackers who are taking advantage of the increasing sophistication and availability of electronic means of theft. As Tim Shimeall, an analyst at Carnegie

Figure 1: Number of trade-secret decisions by year in U.S. federal courts

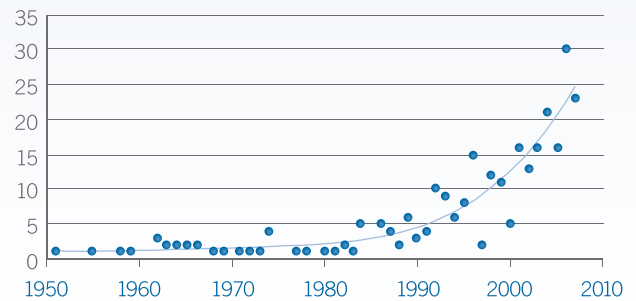
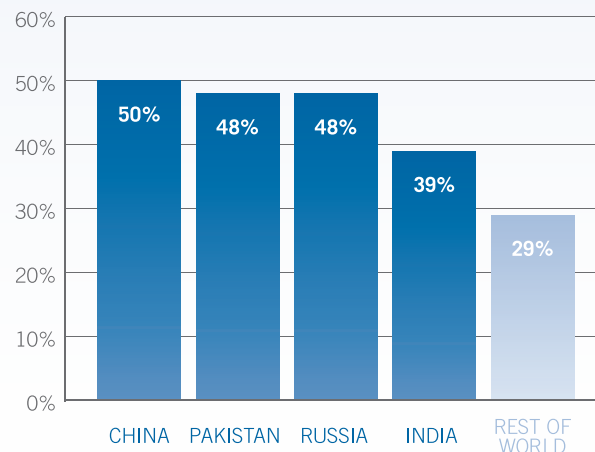


Figure 2: Percentage of respondents stating that the threat level in this country is high



Mellon University’s CERT Network Situational Awareness Group, put it, “With more sophisticated technologies at their fingertips and increased access to data, it has become easier for current employees, contractors, consultants, suppliers, and vendors to steal information.”²⁰

Trade secret theft can have devastating effects on companies’ competitiveness.

Although trade secrets and sensitive corporate data are at risk everywhere, a significant amount of the misappropriation is driven by the fact that sensitive corporate information and technology are being targeted by foreign intelligence services, private companies, academic and research

75% of most organizations' value and sources of revenue creation are in intangible assets, intellectual property and proprietary competitive advantages.

institutions, and citizens. In one survey, U.S. firms were asked to report on suspected, unsuccessful, or successful attempts to compromise or gain unauthorized access to proprietary or trade secret information. Of incidents where the nationality of the primary beneficiary of the theft was known, foreign individuals, firms, and governments were identified as the beneficiary about 70 percent of the time.²¹ In another survey, global firms were asked to indicate countries where digital assets were most at risk. As shown in Figure 2, the firms reported that threat levels were higher in China, Pakistan, Russia, and India than in the rest of the world. Among the factors the respondents cited were issues such as corruption among police and judicial officials, lack of legal protections for intellectual property, weak data privacy protections, and the presence of cybercriminals.²²

The International Trade Commission (ITC) estimates that misappropriation of trade secrets in China cost the U.S. IP-intensive economy \$1.1 billion in 2009.²³ Given that Chinese industrial espionage focuses on “systems, designs, and materials,”²⁴ it is no surprise that the sectors most affected by Chinese trade secret theft are chemical manufacturing, consumer goods, high tech, and heavy manufacturing.²⁵ But the ITC warns that “all sectors are susceptible.”²⁶

That certain Chinese entities are aggressively and systematically stealing proprietary corporate data is well-known in the manufacturing industry. As recounted by a former executive of a leading global contract manufacturer:

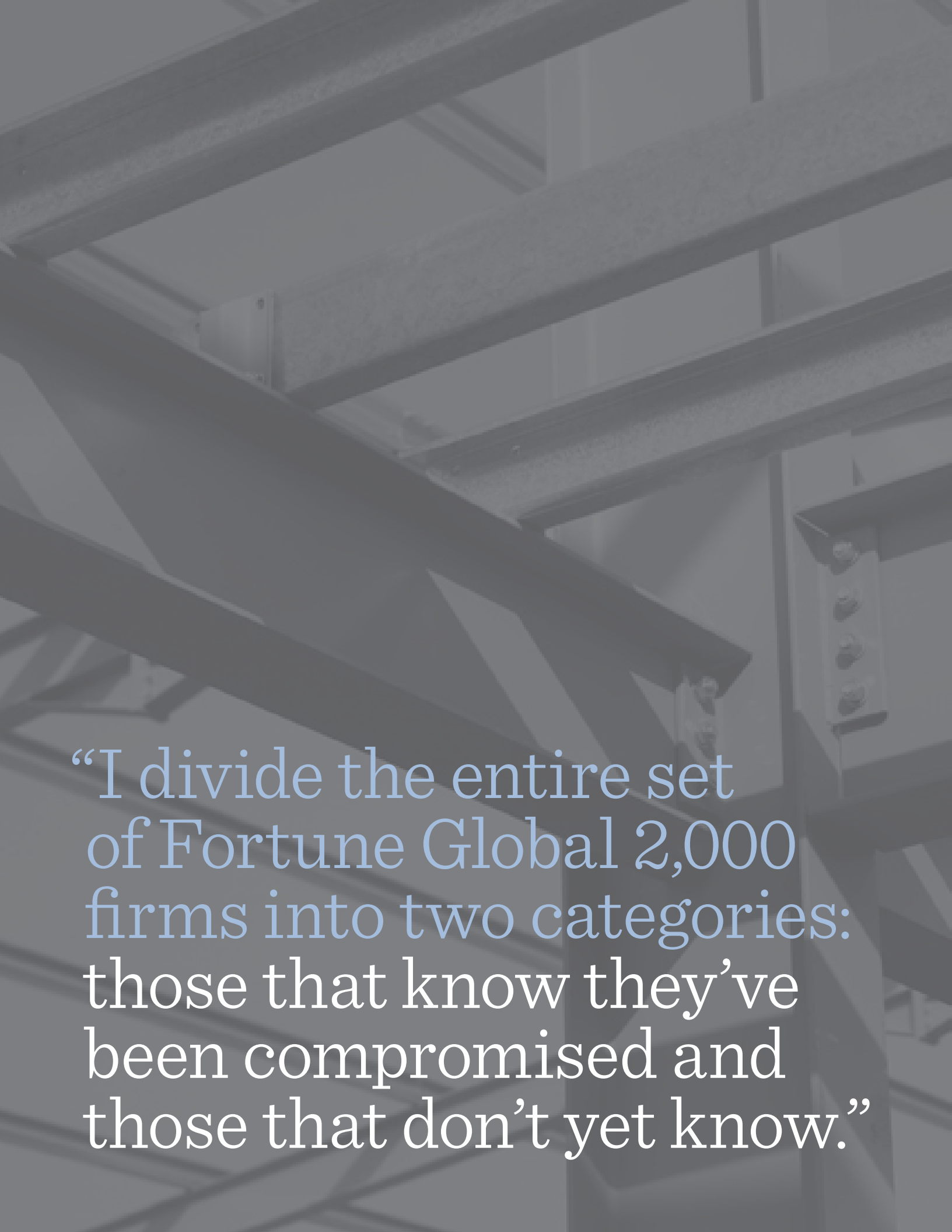
A couple of years ago, a leading contract manufacturer established a manufacturing center for medical devices in Singapore. They chose that location for several key reasons—strong logistics, access to relatively affordable talent and a strong legal and cultural infrastructure of data protection. Clients of this manufacturer had made themselves perfectly clear—they wanted the lowest total landed cost, but were simply not willing to risk

losing their IP by having the key components of their devices manufactured in China. Make the boxes and commodity pieces in China—but build the brains and do final assembly in Singapore, even though it meant significantly higher costs.²⁷

The experience of Massachusetts-based American Superconductor (“AMSC”) illustrates why these precautions are necessary. AMSC makes software, design, and hardware solutions for wind turbines. Its top customer, China-based Sinovel Wind Group, paid an AMSC engineer to steal proprietary source code from AMSC’s secure server in Austria.²⁸ After Sinovel acquired the source code, it began inexplicably turning away AMSC’s shipments. Sinovel had previously provided more than 70 percent of AMSC’s revenues, so the impact on AMSC was devastating. When AMSC announced that Sinovel had stopped making purchases, its stock value plummeted 40 percent in a single day. The theft and the broken business relationship with Sinovel has reduced AMSC’s profits and forced AMSC to cut jobs.²⁹

Trade secret theft occurs everywhere. Less than three months after California-based Jolly Technologies set up an R&D center in India, an Indian employee was caught uploading proprietary Jolly source code and confidential design documents to her personal web-based email account so that she could ship the files out of the research facility.³⁰ In September 2011, DuPont was awarded nearly \$1 billion in damages after a jury found that South Korea’s Kolon Industries hired former DuPont employees to steal confidential data related to Kevlar body armor. A DuPont executive described Kolon’s actions as a “well orchestrated, concerted” campaign that impinged on 40 years and tens of millions of dollars of investment.³¹

Moreover, a single attack can affect companies worldwide. For example, between July and September 2011, Symantec documented a cyberattack against numerous companies involved in the development and production of chemicals



“I divide the entire set of Fortune Global 2,000 firms into two categories: those that know they’ve been compromised and those that don’t yet know.”

\$50 million

in estimated losses were suffered at an American automaker after a former employee copied 4,000 documents onto an external hard drive and went to work for a competitor.

and advanced materials. The attackers were apparently targeting design documents, formulas, and manufacturing processes, and doing so on a global scale: they were able to compromise the computers of organizations headquartered in Belgium, Denmark, Italy, Japan, the Netherlands, Saudi Arabia, the United Kingdom, and the United States.³²

Trade secret theft is a worldwide concern. In the field of high-speed rail technology, both Japanese and European companies claim that Chinese joint-venture partners stole technical secrets to build up their own competitive position. According to an executive at French engineering group Alstom, “Around 90 percent of the [high speed rail] technology the Chinese currently are using is derived from their partnerships or equipment developed by foreign companies.”³³ In 2005, German-based Siemens joined with China National Railway (CNR) to build trains for China’s first high-speed railway. Siemens provided technology to CNR, trained 1,000 CNR technicians in Germany, and set up production facilities in China. China’s next major project, a \$5.7 billion contract to build a high-speed railway between Beijing and Shanghai, was awarded directly to CNR, with Siemens demoted to a subcontractor role. Japan’s Kawasaki Heavy Industries similarly found itself competing directly with its former Chinese junior partner. As a senior Kawasaki executive put it, “How are you supposed to fight rivals when they have your technology, and their cost base is so much lower?”³⁴

A survey of 625 Japanese manufacturing firms in late 2007 found that more than 35 percent of the respondents had

experienced some form of technology loss. More than 60 percent of those leaks involved Chinese actors.³⁵ Japanese firms, one-time leaders in outsourcing manufacturing, are now protecting their “technological crown jewels” by utilizing domestic manufacturing facilities and employing stringent security measures. When Sony announced plans to add manufacturing capacity in China, it made clear that certain key components such as the chip for its PlayStation game console would continue to be produced in Japan, in part to protect Sony’s technology.³⁶ Sharp has taken even more extreme measures to protect its LCD televisions: it bans factory visits, keeps the identities of key engineers private, prohibits employees from bringing camera-equipped cellphones into the plant, and foregoes patent protection on certain products if the patent application would give competitors clues about the technologies involved.³⁷

A German counterintelligence official for the state of Baden-Württemberg estimated in 2009 that German companies were losing around €50 billion and 30,000 jobs to industrial espionage every year. The sectors most under attack included “car manufacturing, renewable energies, chemistry, communication, optics, x-ray technology, machinery, materials research, and armaments. Information being gathered was not just related to research and development but also management techniques and marketing strategies.”³⁸ In both France and South Korea, policymakers have expressed concerns that existing domestic laws protecting trade secrets are insufficient and have proposed legislation to help mitigate the effects of economic espionage.³⁹



When multinational corporations (MNCs) outsource part of their operations, they by necessity are forced to share highly sensitive and valuable trade secrets. Foreign subsidiaries, joint-venture partners, and third-party vendors often need customer lists, internal standards, manufacturing processes, information on sources of goods, recipes, or production and sales strategies in order to carry out their operational responsibilities.⁴⁰

For knowledge-based outsourcing involving specialized domain expertise (e.g., research and development, financial analysis, data mining, engineering and design, graphics simulation, medical services, and clinical trials), the company is invariably required “to disclose and share knowledge-intensive processes with the offshore provider, which knowledge may be in the form of proprietary technology, software, chemical entities, specifications, product designs, business processes, methodologies, drug formulations or other sensitive data.”⁴¹

Although the largest threat to proprietary information comes from current and former employees, a survey of U.S. firms also identified “exploitation of trusted relationships by vendors, customers, joint venture partners, and subcontractors/outsourced providers” as a primary risk to information assets.⁴² These kinds of data security incidents are also among the most costly: another survey of American, European, Australian, and New Zealand firms found that companies spent an average of \$362,269 for each incident in which a supply chain or business partner abused its privileges and obtained data that it should not have had access to. This figure encompasses concrete costs such as out-of-pocket investigation expenses, forensic consulting, fines, and legal fees; it does not include lost labor or productivity costs.⁴³

Moreover, even in situations where the third-party business partner is acting in good faith, the mere fact that a third party has access to the company’s trade secrets increases the risk that they will be compromised. Experts have identified at least 19 other ways, besides deliberate exploitation of trusted business relationships, in which proprietary corporate data can be compromised.⁴⁴ Unless the third party has strong protections in place, any of these 19 other types of threats could result in loss of the company’s trade secrets.

The three major categories of sourcing transactions—captive sourcing, third-party sourcing, and joint-venture sourcing—present varying degrees of risk for companies’ intellectual property. As detailed below, however, all three have resulted in the expropriation of valuable corporate trade secrets in the past.

Captive sourcing offers the most operational control, but even captive sourcing can create vulnerabilities.

Many companies choose to use captive sourcing—that is, building or acquiring their own operations offshore—in order to retain greater control over day-to-operations and corporate intellectual property. Although captive sourcing solutions generally take a long time to implement and require high startup investments, one observer of the Indian outsourcing market has advised that companies “should seriously consider a ‘captive sourcing’ strategy if the sourcing scope involves a substantial transfer to an offshore location of the [company’s] IP ‘crown jewels’ or other mission-critical proprietary technology or data and if the enterprise cost of possibly losing control over some meaningful component of any of those assets is high.”⁴⁵

However, even captive sourcing is not without risk. For example, New York-based chemical maker SI Group Inc. opened a Shanghai factory shortly after the turn of the millennium to produce the company’s signature tackifier resins, which play an important role in the tire-making process. SI Group has since filed suit in China alleging that the former plant manager—the person entrusted with the formula—was hired away by a Chinese competitor, Sino Legend, who now makes a virtually identical product. A judicially-authorized technology

\$362,269

The average cost incurred by companies per incident in which a supply chain or business partner exploits its access to data. Costs include investigation expenses, forensic consulting, fines, and legal fees; it does not include lost labor or productivity costs.

verification center has confirmed similarities between the products offered by SI Group and Sino Legend, as well as similarities in the manufacturing processes and equipment utilized by both companies. SI Group estimates that it has spent more than \$1 million pursuing civil litigation in China after Chinese authorities refused to act: the Shanghai police dropped their investigation in 2009, citing a lack of evidence. Although SI Group is still planning to expand its operations in China and just announced plans to build a \$30 million facility in Nanjing, SI Group's chief executive noted, "We're taking a risk. We have to be careful what level of technology we put here."⁴⁶

A similar problem occurred at GM Daewoo, the South Korean subsidiary of General Motors. According to press accounts, Russian automaker TagAZ hired away two former GM Daewoo engineers, who were later arrested for stealing information about engine and parts designs and other key technology used in one of GM Daewoo's sedan models. TagAZ reportedly used the data to develop and launch its C-100 model in Russia. GM Daewoo eventually was able to obtain a court injunction that banned TagAZ Korea from using or passing on trade secrets and from producing or selling components of the C-100 sedan.⁴⁷

Third-party sourcing offers the greatest flexibility, but it also entails the most exposure.

On the opposite end of the spectrum from captive sourcing is third-party sourcing, or contracting with unaffiliated offshore suppliers. Third-party sourcing offers the advantages of comparatively low startup costs, rapid implementation,

and greater flexibility in growth and termination. But it also requires companies to relinquish more control, including some degree of control over the intellectual property involved in the transaction. The company becomes more dependent on the foreign country's legal regime and timely enforcement of contractual rights.⁴⁸

In one recent demonstration of how third-party sourcing can expose a company's trade secrets, three Chinese citizens were sentenced to prison for collaborating to steal information from Apple's supplier Foxconn. A former and then-active employee of Foxconn were paid for information and images of the iPad 2 so that a Chinese electronics-accessories manufacturer could make protective cases for the iPad 2 several months before the product's release. The Foxconn employee was offered 20,000 yuan (about \$3,000) to steal information on the iPad 2's casing design; the R&D connected with the stolen trade secret is estimated to be worth 100 times that amount.⁴⁹

Problems have also arisen in connection with outsourcing in India. In 2002, an ex-employee of an Indian vendor, Geometric Software Solutions Ltd., was caught attempting to sell \$50 million worth of software source code owned by Geometric Software's U.S.-based client, SolidWorks. The ex-employee had been given access to the proprietary source code as part of a debugging project while he was employed at Geometric Software, and he took the code with him when he left the company. Shortly thereafter, he began emailing SolidWorks' U.S. competitors with offers to sell the code for \$200,000. The ex-employee was caught in a sting operation, but he could not effectively be prosecuted under Indian law:

the source code belonged to SolidWorks, meaning that the ex-employee technically did not steal from his employer, and India does not recognize misappropriation of trade secrets. He was instead charged with simple theft, and was still working as a programmer four years after the charges were filed.⁵⁰

In some instances, a company's trade secrets can be inadvertently compromised by the third-party vendor. For example, an Indian software developer looking to improve a client's code posted some of the code online to seek input from the development community, not realizing that this action compromised the client's proprietary information.⁵¹

Joint-venture sourcing is often perceived as a middle ground, but local partners have used joint-venture vehicles to steal their foreign partners' business secrets.

Joint-venture sourcing, in which foreign companies partner with local entities to share control of local operations, provides a middle approach. The advantages of joint-venture sourcing are that each party can reduce its startup costs and share risks. However, joint ventures also create more complicated structural and operational issues, and the particular laws of the offshore jurisdiction must be carefully considered.⁵² In China, for example, cross-border

An employee was offered 20,000 ¥ (about \$3,000) to steal information on a product design; the R&D connected with the stolen trade secret is estimated to be worth 100 times that amount.

technology license arrangements are governed by the Ministry of Commerce's Technology Import and Export Regulations. Under these regulations, any improvements to the technology belong to the party making the improvement, and no restrictions may be placed upon the licensee's improvements to the technology or use of those improvements.⁵³ In practice, this means that the Chinese partner may be free to develop derivative works based on the licensed technology and claim ownership of the derivative works.

In some cases, trade secrets have been lost before production even began, because local design firms leaked proprietary information about the design of the production facility. According to an industry interview conducted by the ITC, U.S. companies are sometimes required to partner with a Chinese design firm when building a new production facility in China, and "some design firms reportedly have no qualms about disclosing those secrets to the [U.S.] firm's competitors."⁵⁴

The experience of Fellowes, Inc., provides one example of a foreign partner using the guise of a joint venture to steal finished goods, engineering know-how, and proprietary manufacturing production equipment. Illinois-based Fellowes is a market-leading manufacturer of paper shredders and

other office machines. In 2006, Fellowes established a joint venture with Jiangsu Shinri Machinery Co. to set up a production facility in Changzhou, China. After a change in ownership at Shinri, the company insisted that Fellowes assign ownership of the production tools to the joint-venture, sign over its engineering capability and Chinese sales division, inject another \$10 million of capital, and accede to a 40 percent price increase. When Fellowes refused these demands, Shinri locked the 1,600 joint-venture employees out of the production facility; placed security guards at the facility gates to prevent removal of production tools and nearly 70,000 finished shredders; transferred joint-venture funds to a Shinri-controlled bank account; and, under cover of night, drove a truck into the facility and stole several Fellowes-owned injection molding machines, in violation of a court preservation order. Judicial proceedings have been initiated to liquidate the joint venture and auction all of its assets, which will allow Shinri to purchase the remaining equipment, real estate, molding tools, and unshipped shredders—including tools and shredders that embody Fellowes' engineering expertise and intellectual property—at a steep discount. Shinri intends to compete directly with Fellowes in the shredding business, and in fact has already begun to market shredders to potential buyers in Europe. Fellowes estimates that its cumulative economic loss from Shinri's actions exceeds \$100 million.⁵⁵

\$100 million

in economic loss was suffered by an American manufacturer that partnered with an international manufacturer that then used the guise of a joint venture to steal finished goods, engineering know-how, and proprietary manufacturing production equipment.

In some cases,
trade secrets have been
lost before production
even began, because
local design firms leaked
proprietary information
about the design of the
production facility.



3.

THE WEAK RULE
OF LAW IN MANY
COUNTRIES MAKES IT
ALL BUT IMPOSSIBLE
FOR MNCs TO ADDRESS
TRADE SECRET THEFT
AFTER THE FACT.

Divergence in trade secret laws across various geographies, the difficulty of achieving effective enforcement, and conflicts of national interests make trade secret protection a complicated issue for multinationals and organizations with a global supply chain.

Moreover, once theft occurs, it is virtually impossible to remedy the resulting economic and competitive damage through traditional enforcement mechanisms.

Outside the United States and some countries in Europe, trade secret protections are often weak.

In the United States, trade secrets are protected by both federal and state statutes, and the penalties for misappropriation include criminal sanctions, actual and punitive damages, injunctive relief, and attorneys' fees. Most countries in the European Union also outlaw trade secret theft in some way, whether through criminal sanctions, specific civil legislation, or more general unfair competition rules, tort law, labor law, breach of confidence actions, or contractual claims.⁵⁶

By contrast, a number of other jurisdictions—including India, Singapore, Malaysia, and Hong Kong—do not provide statutory protection for trade secrets or confidential information.⁵⁷ Moreover, contractual protections are of limited enforceability.

For example, although India recognizes a common-law tort of “breach of confidence,” the tort cannot always be utilized in the global sourcing context because the duty of confidence exists only when the misappropriator has a fiduciary or employer-employee relationship with the complaining party.⁵⁸ Companies that outsource to India therefore rely primarily on contracts to protect their trade secrets—and even then, there are legal barriers to effective enforcement. For example, India generally does not permit third-party beneficiaries to enforce contract terms. If an

Indian vendor enters into a contract with an MNC to provide services to both the MNC and one of the MNC's affiliates, it is doubtful under Indian law whether the affiliate would have standing to enforce the contract.⁵⁹

Although it is standard practice to specify that confidentiality provisions survive termination of the outsourcing agreement, some countries limit the enforceability of such provisions.⁶⁰ Similarly, noncompete provisions after termination of the agreement may not be enforceable.⁶¹ Chinese law permits noncompete provisions to survive for up to two years after dissolution or termination of the employment contract, but noncompete agreements must be supported by additional consideration and are only applicable to senior managers, senior technical personnel, and other personnel with confidential obligations.⁶²

Brazil is becoming a world player in information technology outsourcing: numerous leading technology and consulting companies have outsourced IT work or set up captive research centers there.⁶³ However, trade secrets are also at risk in Brazil. The legislature criminalized trade secret theft in 1996, but the remedies for breach are limited. The statute stipulates that the penalty upon conviction is three to 12 months imprisonment or a fine, and the availability of injunctive relief is uncertain. Moreover, Brazil's judicial system is generally regarded as dysfunctional, primarily because of undue delay, corruption, and poor-quality decisions. One practitioner has concluded that in Brazil, “trade secret protection is poorly established and business cannot rely on the judicial system to adequately support the law regarding trade secret protection.”⁶⁴

Challenges in the Indian judicial system include a backlog of cases, hand-kept records, misplaced filings and wide acceptance of adjournments due to absentee parties and witnesses.

Where laws do exist, local courts often have a poor track record of enforcement.

Although China has a comprehensive set of laws and regulations designed to protect trade secrets, in practice neither criminal nor civil enforcement has proven effective for MNC trade secret owners. The most prominent criminal cases brought by the Chinese government have been against foreigners; in fact, the ITC's research did not identify any criminal cases that were undertaken at the request of U.S. firms.⁶⁵ After Shinri shut down the joint venture facility with Fellowes as described earlier, Fellowes' CEO traveled to China and met with local government officials. In his words, "They sympathized with our plight but were either unable or unwilling to force our Chinese partner to open our factory and they were unable to facilitate a purchase of the joint venture by Fellowes."⁶⁶

Civil litigation in China rarely provides effective relief for trade secret theft. According to the European Union Chamber of

Commerce in China, European companies doing business in China face "substantial risks" of trade secret infringement but often find it "very difficult" to enforce their rights in Chinese courts.⁶⁷ In the ITC's survey, only 0.6 percent of U.S. firms that reported material losses due to trade secret misappropriation between 2007 and 2009 pursued civil proceedings in China.⁶⁸ Misappropriation is difficult to prove, because there is no U.S.-style discovery and the evidentiary burden for the plaintiff is daunting: oral testimony is often considered insufficient, so "written evidence that a defendant agreed to treat particular information as a trade secret, that he or she received the confidential information, and that the information was disclosed may all be required to successfully state a claim."⁶⁹ Although injunctive relief is available and investigation expenses can be included in the claim for damages, most damage amounts have been low and therefore have little deterrent effect.⁷⁰

India's enforcement mechanisms for intellectual property rights have also been criticized, primarily due to the

inefficiency of the Indian judicial system. There is a substantial backlog of cases, court records are kept by hand, filings are often misplaced, courts take numerous adjournments due to the unavailability of parties or witnesses, cases are frequently shuffled between multiple judges, and respondents have the ability to drag out the case.⁷¹ In addition, the remedies are viewed as inadequate to provide redress and deter future violations: judgments are difficult to enforce, monetary damages are hard to prove and are generally meager, no punitive damages are available, and the lack of statutory trade secret protection makes injunctive relief harder to obtain.⁷²

In a survey of global firms, Pakistan, China, and Russia (in that order) were identified as having the worst reputation for pursuing or investigating security incidents involving breaches of corporate data. The top reasons for these countries' poor reputation ratings were corruption among law enforcement and the legal systems, as well as poor skills among law enforcement.⁷³

In some countries, the government may be condoning, facilitating, or even participating in the trade secret theft.

Governments have historically pressured foreign firms to reveal trade secrets and technology as a condition of doing business locally, and the practice continues to this day. In the 1970s, the Indian government demanded that Coca-Cola either turn over 60 percent of its Indian subsidiary to Indian shareholders and divulge the secret formula for its signature soft drink, or end operations in India. Coca-Cola at that time had been doing business in India for 25 years, but the company chose to abandon its investment in India—and India's lucrative market of 550 million potential consumers—rather than disclose its trade secrets.⁷⁴

In a more recent example, the Chinese government has been placing pressure on foreign automakers to reveal engineering technologies related to electric vehicles. After General Motors began preparations to sell its plug-in hybrid vehicle, the Volt, in China, the Chinese government refused to allow the Volt to qualify for consumer subsidies totaling up

to \$19,300 per car unless GM agreed to transfer engineering secrets to a joint venture with a Chinese automaker. The Chinese government specified that at least one of three core technologies—electric motors, complex electronic controls, or power storage devices relating to batteries or fuel cells—would need to be included in the technology transfer in order for the vehicle to be eligible for the subsidies. GM later announced that it would sell the Volt without attempting to qualify for the subsidy.⁷⁵

There is also evidence that certain Chinese government officials and state-owned enterprises (SOEs) have been involved in trade secret theft. Chinese SOEs were reported to be responsible for 6.5 percent of trade secret misappropriation in China between 2007 and 2009, primarily affecting the high-tech and heavy manufacturing sectors.⁷⁶ A criminal indictment handed down in February 2012 alleges that Walter Liew conspired to steal DuPont's trade secrets relating to production technology for titanium dioxide, which is a commercially valuable white pigment used in a large number of materials ranging from paints to paper. According to documents filed in the case, Liew told others that he had been tasked by Chinese intelligence officials to seek titanium dioxide technology. A Chinese SOE and three of its subsidiaries are also named as defendants in the case. The indictment alleges that Liew provided confidential information about DuPont's technology to these SOEs, who specifically asked Liew for DuPont blueprints and the names of former DuPont employees who would work on their project.⁷⁷

Regardless of whether governments are actively participating in trade secret theft, government regulations can have the effect of making proprietary corporate information more vulnerable. For example, Chinese patent regulations that went into effect in 2010 now require all patent applicants who complete inventions in China to apply for security clearance before applying for patents abroad. Because the security examination can take up to six months, an attorney in Beijing has noted that the delay extends the period during which people can access the information or copy it before the invention is patented—thereby increasing the risk of trade secret theft.⁷⁸



4.

PROACTIVE MEASURES
MUST BE IMPLEMENTED
ACROSS ORGANIZATIONS
TO PREVENT RAMPANT
TRADE SECRET THEFT.

Protecting trade secrets is challenging. In the ITC's study, almost all of the firms that experienced trade secret misappropriation in China had taken some steps to protect their trade secrets. Nonetheless, the vast majority (85 percent) of these firms reported that the steps were ineffective.⁷⁹

For example, companies found that they could not rely solely on nondisclosure agreements: former employees often took information to new employers or used the information to start rival companies, despite having signed nondisclosure agreements.⁸⁰

In the Internet era, companies can no longer rely on containment strategies to deal with information compromises, nor can they assume that confidentiality obligations alone will be sufficient to deter or remedy theft. Given the speed at which information-based assets can now be acquired and disseminated globally, post hoc attempts to contain the damages or extent of the loss are seldom effective. As security organization ASIS International explains:

Today, the value and competitive advantages routinely found in an organization's information assets—many of which may be targeted for possible compromise—can be quickly discerned and extracted, in whole or part, and instantaneously distributed to a growing labyrinth of skilled and organized information brokers, counterfeiters, and/or economic-competitive adversaries. The consequences in terms of lost economic/competitive advantage can be extremely quick and long lasting.⁸¹

Moreover, companies' existing information security measures are rarely adequate to prevent cyberattacks. A 2011 report showed that 73 percent of companies surveyed had been hacked via their web applications within the past 24 months; nonetheless, 88 percent of them spent more money on coffee than on securing their web applications.⁸² According to another study, "just 13 percent of companies have a cross-functional cyber risk team that bridges the technical, financial, and other elements of a company."⁸³

Proactive risk mitigation measures are particularly important for companies operating in foreign countries where the legal remedies and enforcement mechanisms for trade secret misappropriation are limited.⁸⁴ As two practitioners have observed, "prevention is the best protection when it comes to trade secrets."⁸⁵ To protect themselves, companies should: (1) conduct a strategic assessment of their trade secrets, (2) undertake appropriate precontractual due diligence, (3) employ strong contractual protections, backed by enforceable audit rights and penalties, (4) utilize appropriate operational and security measures, and (5) take appropriate action after the business relationship has ended.

73% of companies surveyed had been hacked via their web applications within the past 24 months; 88% of them spent more money on coffee than on securing their web applications.

1. Strategically assess the company's trade secrets.

As part of their strategic assessment, companies should:

Establish an internal trade secrets policy that identifies what information the company deems confidential, includes a process for ensuring continuity in the classification of new trade secrets, and spells out the consequences for improper use or disclosure of confidential information.

Integrate the internal trade secrets policy into the company's supplier code of conduct, to set out clear expectations that suppliers will protect the company's trade secrets.

Consider which trade secrets should be transferred to suppliers. Practitioners advise that companies should “be extremely particular about which IP must truly be licensed or otherwise transferred ... and avoid where possible transferring ... ‘crown jewels’ or technology that is core or critical” to business operations.⁸⁶ The evaluation should take into account the sensitivity of the IP at issue, the effectiveness of the legal protections available in the country where the supplier operates, whether the rule of law is strong in that jurisdiction, and whether the company's business needs can be met by transferring only some of the company's trade secrets.

For example, the chairman of Central Japan Railway, one of Japan's largest high-speed train operators, is so concerned about technology theft in China that he has prohibited his company from bidding on contracts there.⁸⁷ Owens-Illinois Inc., an Ohio bottle-maker, plans to invest millions of dollars in Chinese acquisitions and joint ventures in the coming years but will reserve key trade secrets for its U.S. labs. According to Owens-Illinois' president of global glass operations, his company can succeed in China by introducing “the basic stuff.”⁸⁸

Consider how best to structure operations to minimize vulnerabilities.

Many companies prefer to structure joint ventures so that their own employees are in charge of running the plant, or at least have key roles in managing the intellectual property at issue. That same desire for more control is also driving some firms to seek majority stakes in joint ventures when possible. For instance, Connecticut-based construction equipment manufacturer Terex Corp. has been establishing joint ventures in China since the 1990s, but Terex's chief executive now prefers to strike deals that give Terex majority control—in part because he feels that majority ownership provides better intellectual property protection.⁸⁹

Other firms avoid joint ventures entirely. Cree, a North Carolina-based manufacturer of light-emitting diodes (LEDs), makes its LED wafers in the United States, then ships the wafers to China for insertion into its products. Cree owns its Chinese manufacturing facility outright, rather than operating it in conjunction with a joint venture or partner. Cree acquired the plant in 2007, when it bought a Chinese company that had been one of Cree's customers. The Chinese company at the time comprised 1,300 employees and a manufacturing facility. “We wanted to control the tech and distribution of the tech and control the IP associated with that,” Cree's CFO told the *Wall Street Journal*. “The best way to do that is with a team we knew for a number of years and be able to control the whole venture.”⁹⁰

Segmenting the manufacturing process—either among multiple suppliers or across different locations—is another way of ensuring that the company's intellectual property is not concentrated in one place for thieves to steal. For example, one Western appliance manufacturer decided to make electric motors and electrical cords in China, but send all the components to a plant in Mexico to be assembled. According to a consultant who worked with the manufacturer, the company did so in order to ensure that “nobody in there had all of the capabilities to actually make that refrigerator and start selling it.”⁹¹

2. Conduct appropriate due diligence before entering into any contract.

In connection with their due diligence efforts, companies should:

Conduct an assessment to ensure that potential suppliers are able to adequately protect the company's trade secrets. This process should include preparation of a detailed checklist that maps to requirements in the company's supplier code of conduct, including the requirements specifically related to the company's trade secret policy, and a thorough assessment that examines all of the issues on the checklist.

Evaluate other IP-related issues, not just the supplier's performance track record and financial condition. It is useful due diligence to determine if the supplier has a reputation for intellectual property rights violations, trade complaints, or export-control issues; has links to other firms with these issues; or has ties to foreign governments that have a history of disregarding intellectual property rights. These are red flags meriting further investigation. In situations involving core technologies, companies may want to undertake more extensive due diligence, such as an undercover investigation to see whether the supplier is willing to violate others' IP rights—a warning sign that the supplier is also likely to be cavalier about protecting the company's trade secrets.

Scrutinize the supplier's employment and nondisclosure agreements. Companies should ensure that the supplier has written employment and nondisclosure agreements in place with its employees and consultants. Additional scrutiny may be advisable to verify that these agreements are adequate to protect the company's rights and interests, and that the agreements are enforceable under the laws of the host country.

Perform due diligence with respect to the supplier's subcontractors, if possible. The actions of subcontractors can pose a grave—and often unanticipated—risk to companies' sensitive information. The University of California San Francisco Medical Center (UCSF) was contacted by a Pakistani medical transcriber, who threatened to post patients' confidential files online unless she received the back pay she was owed. Hospital officials eventually figured

out how the files had ended up in Pakistan: UCSF has long outsourced a portion of its transcription work to a California company, which in turn subcontracted work to a Florida woman, who—despite a no-subcontracting restriction in her contract—farmed out work to a Texas man, who in turn sent work to the Pakistani transcriber. The Pakistani woman was subsequently paid and she promised to destroy all UCSF files in her possession, but, as press accounts noted, “there's no proof that she's made good on that promise.”⁹²

3. Ensure that strong contractual protections are in place.

The company's contract with the supplier should ensure strong protections for the duration of the business relationship and afterward. For example, the contract provisions should clearly identify the information that the company deems confidential; prohibit the wrongful disclosure and misappropriation of trade secrets by the supplier, its employees, and its subcontractors; require the supplier to restrict, monitor, and (where appropriate) record access to the company's confidential information; and specify that the company has a right to audit for compliance. Upon termination of the agreement, the supplier should be required to return all trade secrets to the company and continue to honor its confidentiality obligations.

The contract should also make clear that the company has the right to enforce violations of the contractual provisions, obtain damages for breach, and seek injunctive relief. Although it may not be possible to avoid altogether the application of foreign trade secret laws through a governing law clause,⁹³ some experts recommend specifying that trade secret and other IP disputes are to be resolved through confidential mediation or arbitration in a convenient and trusted jurisdiction rather than litigation in the local courts. As one practitioner has warned, “in many offshore jurisdictions trade secret litigation can lead to the open disclosure and consequential loss of the trade secrets at issue if the legal proceedings are not closed.”⁹⁴ Moreover, mandatory mediation or arbitration can sometimes help avoid the delays, inefficiencies, and risk of bias and corruption that often plague litigation in foreign countries.

Consider entering into agreements directly with the supplier's employees.

Because many jurisdictions in Asia and Latin America do not recognize the concept of third-party beneficiary, companies cannot necessarily rely on being a third-party beneficiary of agreements between suppliers and their employees.⁹⁵ In some cases it may be advisable to investigate entering into confidentiality or nondisclosure agreements directly with a supplier's key employees—e.g., if necessary to ensure that confidentiality obligations remain in force if the employee leaves the supplier and that there is contractual privity to sue in the event of a breach. If local-language agreements are necessary or advisable, bilingual documents should be used where appropriate, and copies kept on file. Where possible, the relevant agreements might be executed by all three parties: the company, the supplier, and the supplier's relevant employee.

Consider contractual protections against misconduct by the supplier's subcontractors.

If subcontractors are likely to have access to the company's proprietary information, the company should ensure that its contract with the supplier contains appropriate safeguards. For example, the company may want to retain prior approval rights with respect to subcontractors, retain the right to review the terms of subcontracts, require that IP ownership and confidentiality obligations flow down into subcontracts, and/or require the supplier to be contractually responsible for subcontracted functions. For the same contractual privity reasons discussed above in connection with supplier employees, the company may also want to enter into agreements directly with particular subcontractors of the supplier.

4. Take appropriate operational and security measures during the life of the business relationship.

Build a culture of compliance so that the supplier's employees understand and are able to fulfill their obligations to protect confidential information.

For example, active engagement with the supplier's management personnel can help set the appropriate tone throughout the organization. Supplier employees should be trained on the importance of protecting trade secrets, as well as the supplier's and the company's

relevant codes of conduct, policies, and processes for doing so. Consistent implementation of clear policies on the permitted access, use, and disclosure of trade secrets can similarly help foster understanding and commitment. Employees should also undergo meaningful background checks where advisable and permitted; should be permitted to access the company's trade secrets only on a need-to-know basis; and should be required to sign confidentiality agreements prior to receiving any proprietary information.

Consider appropriate physical security measures to protect trade secrets.

For example, it may be necessary to keep confidential information in restricted or locked areas, with limitations on employees' ability to remove the material from the premises. Many companies mark all trade secret documents and storage media as Classified, Restricted, Confidential, Do Not Disclose, or another label particular to the company's business. Companies may also want to ensure that there are transfer protocols for secure internal storage and routing of confidential information, such as requiring use of couriers or routing information through designated recipients to minimize the number of people with access to the information. Documents should be shredded before disposal. Companies should also ensure security of all office entrances and appropriate restrictions on physical access by visitors (e.g., the use of a log, visitor's pass, escort, or nondisclosure agreement as necessary).

Technological safeguards—which are more important than ever—should also be considered.

A number of U.S. firms are encrypting design plans, with a special code required for access; creating documents that “expire” and cannot be saved, forwarded, or printed; or using “time bomb” files that live for a certain amount of time and then disappear.⁹⁶ Other companies use separate computer systems for sensitive information or keep the computers bearing key information off the Internet. Practitioners have also recommended that companies require the use of sign-in/out logs that identify the individuals accessing the confidential information and for how long; establish policies for transmitting confidential information over communication channels that can be tapped; employ computer use policies that permit monitoring of electronic transmissions so that the company can be alerted if confidential files are being transmitted externally

without the company's consent; and limit or prohibit non-work-related software and portable storage devices.

Systematically engage with the supplier to ensure that these personnel, physical, and technological measures are working effectively. Ideally, companies and their suppliers should be working as partners to protect valuable corporate secrets. More open communication and more active involvement can foster greater trust and a better working relationship between companies and their suppliers. That said, extra security and controls may be needed if the supplier is also doing work for the company's competitors—e.g., physical separation of work spaces where the company's confidential information is used or stored, or measures to ensure that employees who deal with competitors' products are denied access to the company's confidential information.

5. Take appropriate action after the business relationship has ended (both with respect to the supplier and the supplier's employees).

Remind departing employees of their continuing obligation not to disclose trade secrets. Companies should require departing employees to sign a document acknowledging that they had access to confidential information and promising not to disclose or use the confidential materials. Employees should be required to return all confidential materials and electronic storage devices, and their electronic access rights should be terminated immediately upon departure. Companies should also be cognizant of "red flags" raised by ex-employees' activities, particularly if they take employment with a competitor. In such cases, it may be appropriate to give notice to the new employer of the ex-employee's continuing obligation not to disclose trade secrets.

Ensure that former business partners do not leak trade secrets. Many of the same practices can also be important when the company ends its relationship with its supplier. Commitments from the supplier to return and to not use the company's trade secrets can help ensure that the company's trade secrets remain safe, as can reminders of the supplier's ongoing confidentiality obligations.

Concluding Remarks

As more companies look to capitalize on the benefits of expansion to global markets, trade secret theft in global supply chains will continue to grow—in scope, frequency, complexity, and magnitude. To preserve their economic competitiveness, companies whose supply chains extend to countries with weak or no trade secret protection must take proactive measures to safeguard their most valuable trade secrets.

These measures, discussed throughout the paper, work by elevating the importance of trade secret protection in supplier relationships and creating much-needed disincentives for theft. They include:

- (1) conducting a strategic assessment of trade secrets;
- (2) undertaking appropriate pre-contractual due diligence;
- (3) employing strong contractual protections, backed by enforceable audit rights and penalties;
- (4) utilizing appropriate operational and security measures; and
- (5) taking appropriate action after a business relationship has ended.

Companies can begin to implement these tactics and tools to help mitigate the risk of trade secret theft and protect their trade secrets as global operations grow and evolve. The more industry works collaboratively to secure supply chains and business networks, the less vulnerable and more profitable global trade will be for all. ■

ENDNOTES

¹ Dmitri Alperovitch, McAfee, *Revealed: Operation Shady RAT 2* (Aug. 2011), <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

² *Id.*

³ *Trends in Proprietary Information Loss*, ASIS International, 37 (Aug. 2007), <http://www.asisonline.org/newsroom/surveys/spi2.pdf>; see also Forrester Consulting, *The Value of Corporate Secrets* 5 (Mar. 2010), http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf (concluding, based on survey of North American, European, Australian, and New Zealand companies, that “[e]nterprises in highly knowledge-intensive industries like manufacturing, information services, professional, scientific and technical services, and transportation accrue between 70% and 80% of their information portfolio value from secrets”).

⁴ David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonzaga L. Rev. 291, 304-05 & n.62 (2010).

⁵ Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, at 4 (Oct. 2011) [hereinafter ONCIX Report] (“Estimates from academic literature on the losses from economic espionage range... from \$2 billion to \$400 billion or more a year ...”).

⁶ See Matthew Dolan, *Ex-Ford Engineer Pleads Guilty in Trade-Secrets Case*, Wall St. J., Nov. 17, 2010.

⁷ ONCIX Report, *supra* note 5, at 3.

⁸ McAfee, *Unsecured Economies: Protecting Vital Information* 7 (2009), available at <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.

⁹ ASIS International, *supra* note 3, at 38.

¹⁰ McAfee, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency* 15 (2011), <http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf> (concluding, based on a survey of more than 1,000 senior IT decision makers in the United States, United Kingdom, Japan, China, India, Brazil, and the Middle East, that “[a]round a quarter of organizations have had a merger and acquisition or a new product/solution rollout stopped or slowed by a data breach, or the credible threat of a data breach”).

¹¹ Almeling et al., *supra* note 4, at 293, 302.

¹² Hogan Lovells International LLP, *Report on Trade Secrets for the European Commission* 6 (Jan. 2012), http://ec.europa.eu/internal_market/iprenforcement/docs/trade/Study_Trade_Secrets_en.pdf.

¹³ McAfee, *supra* note 10, at 5.

¹⁴ Press Release, Cisco, *Global Internet Traffic Projected to Quadruple by 2015* (June 1, 2011), <http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003>.

¹⁵ ONCIX Report, *supra* note 5, at 7.

¹⁶ McAfee, *supra* note 8, at 18.

¹⁷ McAfee, *supra* note 10, at 3.

¹⁸ *Id.*

¹⁹ McAfee, *supra* note 8, at 19.

²⁰ *Id.* at 9.

²¹ ASIS International, *supra* note 3, at 23.

²² McAfee, *supra* note 8, at 12-16; McAfee, *supra* note 10, at 10 (reporting that China, Russia, and Pakistan were still regarded as the least safe countries for data storage in 2010, and noting that the United Kingdom, Germany, and the United States continued to be perceived as the safest).

²³ U.S. Int'l Trade Comm'n, Pub. 4226, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy* 3-42 (May 2011), <http://www.usitc.gov/publications/332/pub4226.pdf>.

²⁴ U.S. China Economic and Security Review, 2005 Report to Congress 93 (Nov. 2005), http://www.uscc.gov/annual_report/2005/annual_report_full_05.pdf (“According to David Szady, the former chief of FBI counterintelligence operations, ... China’s industrial espionage is focused on systems, materials, and designs and ‘going after both the private sector, the industrial complexes, as well as the colleges and universities in collecting scientific developments that they need.’”); see also Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* 54-55 (2011) (“Chinese attackers are not smash-and-grab criminals, pilfering personal bank accounts and running up fraudulent credit card charges. Their line of work is hard-core cyberespionage, and their targets are the technology, designs, and trade secrets of private companies ...”).

²⁵ U.S. Int'l Trade Comm'n, *supra* note 23, at 3-41.

²⁶ *Id.*

²⁷ McAfee, *supra* note 8, at 15.

²⁸ That Sinovel engaged in industrial espionage is difficult to dispute: AMSC found hundreds of emails between the engineer and Sinovel employees, including one in which the engineer sent AMSC source code to his Sinovel counterpart, as well as a \$1.7 million consulting contract signed by Sinovel's chairman. The engineer was arrested, confessed that he had reprogrammed the source code for Sinovel, and is now serving time in prison for distribution of trade secrets. See Michael Riley & Ashlee Vance, *Inside the Chinese Boom in Corporate Espionage*, BloombergBusinessweek, Mar. 15, 2012, <http://www.businessweek.com/printer/articles/13858-inside-the-chinese-boom-in-corporate-espionage>.

²⁹ See *id.*; Robert D. Atkinson, Info. Tech. & Innovation Found., *Enough Is Enough: Confronting Chinese Innovation Mercantilism* 39 (Feb. 2012), <http://www2.itif.org/2012-enough-enough-chinese-mercantilism.pdf>.

³⁰ John Ribeiro, *Source Code Stolen from U.S. Software Company in India*, ComputerWorld, Aug. 5, 2004, http://www.computerworld.com/s/article/95045/Source_code_stolen_from_U.S._software_company_in_India?nas=SEC2-95045&taxonomyId=070.

- ³¹ Doug Cameron, *DuPont Wins Nearly \$1 Billion in Secrets Case*, Wall St. J., Sept. 15, 2011.
- ³² See Eric Chien & Gavin O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry* (Oct. 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.
- ³³ Peter Marsh & Jennifer Thompson, *Alstom in Spat with Siemens over China Leaks*, Fin. Times, Oct. 31, 2011.
- ³⁴ See Editorial, *China and Intellectual Property*, N.Y. Times, Dec. 24, 2010, <http://www.nytimes.com/2010/12/24/opinion/24fri1.html>; U.S. Int'l Trade Comm'n, Pub. 4199 (amended), *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy* 4-11 (Nov. 2010), <http://www.usitc.gov/publications/332/pub4199.pdf>; Norihiko Shirouzu, *Train Makers Rail Against China's High-Speed Designs*, Wall St. J., Nov. 17, 2010.
- ³⁵ ONCIX Report, *supra* note 5, at B-1.
- ³⁶ Daisuke Wakabayashi & Nathan Layne, *Japan Turning to Patents to Keep Competitive Edge*, Taipei Times, July 8, 2004, <http://www.taipeitimes.com/News/editorials/archives/2004/07/08/2003178161>.
- ³⁷ *Id.*
- ³⁸ Kate Connolly, *Germany Accuses China of Industrial Espionage*, Guardian, July 22, 2009, <http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage>.
- ³⁹ ONCIX Report, *supra* note 5, at B-1.
- ⁴⁰ Daniel Plane, *Protect Your Secrets in China*, Managing IP, Feb. 2009, at 46.
- ⁴¹ Sonia Baldia, *Knowledge Process Outsourcing to India: Important Considerations for U.S. Companies*, 1587 PLI/Corp 171, at *178 (2006).
- ⁴² ASIS International, *supra* note 3, at 12.
- ⁴³ See Forrester Consulting, *supra* note 3, at 9. The cost per incident when supply chain or business partners abuse their privileges is comparable to the cost per incident when rogue employees steal company data (\$362,572); only incidents involving IT administrators abusing their privileges and stealing data are more costly (\$452,238). *Id.*
- ⁴⁴ Those 19 threat vectors are: (1) Inadvertent actions by current or former employees during oral seminar presentations; (2) Inadvertent actions by current or former employees via written material, publications, or handouts; (3) Inadvertent actions by current or former employees via electronically misdirected fax or e-mail; (4) Inadvertent actions by current or former employees via visual observation of written material, desktops, white boards, computer screens, etc.; (5) Deliberate disclosure by current or former employees to unauthorized parties; (6) Unauthorized electronic access/penetration of information systems by current or former employees; (7) Unauthorized physical access to information by current or former employees; (8) Open-source collection of public information; (9) Data mining or software-driven collection and analysis of open-source data; (10) Exploitive social engineering techniques (manipulation of human tendencies such as misrepresentation to obtain passwords, false job interviews, visits to facilities and tradeshow, etc.); (11) Hiring away employees and placing them in positions where they must use trade secrets that they are obligated to protect to do their new job; (12) Extortion or coercion of an unwilling trusted insider by an outsider; (13) Co-opting of an employee or former employee; (14) Co-opting of a company vendor, subcontractor, or outsourced provider employee; (15) Targeting of off-site meeting or conference; (16) Electronic eavesdropping, wiretapping, or interception of communications; (17) Theft of hard-copy information, samples, or prototypes; dumpster diving/theft of trash; (18) Theft of proprietary source code/computer programs; and (19) Intentional unauthorized access/penetration of information systems by outsiders. ASIS International, *supra* note 3, at 28.
- ⁴⁵ Sonia Baldia, *Intellectual Property in Global Sourcing: The Art of the Transfer*, 38 Geo. J. Int'l L. 499, 506 (2007).
- ⁴⁶ James T. Areddy, *In China, Tire-Espionage Suit Treads Loudly*, Wall St. J., Apr. 28, 2011, available at <http://webreprints.djreprints.com/2663120463063.html>; Press Release, SI Group, The Facts Regarding SI Group Tackifier Resins (Mar. 14, 2012), <http://www.siigroup.com/pressrelease.asp?ArticleId=173>.
- ⁴⁷ AFP, *GM Daewoo Files Action Over "Copying," Drive* (Sept. 22, 2009), <http://www.drive.com.au/Editorial/ArticleDetail.aspx?ArticleID=65859&vf=26>; AFP, *GM Daewoo Welcomes Ban on Russian "Copying," China Post*, Oct. 29, 2009, <http://www.chinapost.com.tw/business/company-focus/2009/10/29/230655/GM-Daewoo.htm>.
- ⁴⁸ Baldia, *supra* note 45, at 504, 506.
- ⁴⁹ Michael Kan, *Chinese Court Sentences Three to Prison for iPad Design Leak*, PCWorld, June 16, 2011, http://www.pcworld.com/businesscenter/article/230406/chinese_court_sentences_three_to_prison_for_ipad_design_leak.html.
- ⁵⁰ George W. Reynolds, *Ethics in Information Technology* 84 (3d ed. 2009); *CBI-FBI Team Nabs IIT Engineer for Software Theft*, Rediff (Aug. 28, 2002), <http://www.rediff.com/money/2002/aug/28cbi.htm>.
- ⁵¹ McAfee, *supra* note 8, at 16.
- ⁵² Baldia, *supra* note 45, at 505.
- ⁵³ See Administration of Technology Import and Export Regulations, Art. 27, <http://tradeinservices.mofcom.gov.cn/en/i/2007-01-07/3546.shtml> ("During the valid term of a technology import contract, the fruits of improvements to the technology shall belong to the party making the improvements."); *id.* Art. 29 ("A technology import contract may not contain any of the following restrictive clauses: ... 3. restricting the licensee from making improvements to the technology provided by the licensor or restricting the licensee from using improved technology.").
- ⁵⁴ U.S. Int'l Trade Comm'n, *supra* note 34, at 4-11.
- ⁵⁵ See Asia Overview: Protecting American Interests in China and Asia: Hearing Before the Subcomm. on Asia and the Pacific of the H. Comm. on Foreign Affairs, 112d Cong. 35-42 (2011), <http://foreignaffairs.house.gov/112/65495.pdf> (statement of James Fellowes, Chairman and CEO, Fellowes, Inc.); see also Press Release, Office of U.S. Sen. Dick Durbin, Durbin Meets with Fellowes, Inc CEO to Discuss Dispute in China (Mar. 31, 2011), <http://durbin.senate.gov/public/index.cfm/pressreleases?ID=b34cb20b-7f45-40ba-8b8e-e4c0eb32677c>.
- ⁵⁶ See Hogan Lovells, *supra* note 12, at 36-39.
- ⁵⁷ Baldia, *supra* note 45, at 510-11.
- ⁵⁸ *Id.* at 511.
- ⁵⁹ Sonia Baldia, *Navigating Cross Border Legal Risks in Intellectual Property Licensing and Technology Transfer to India*, 1815 PLI/Corp 229, at *265-68 (2010).

- ⁶⁰ See Harry Rubin, *Supply-Side/Manufacturing Outsourcing – Strategies and Negotiations*, 38 Geo. J. Int'l Law 713, 727 (2007).
- ⁶¹ *Id.* at 728.
- ⁶² J. Benjamin Bai & Guoping Da, *Strategies for Trade Secrets Protection in China*, 9 Nw. J. Tech. & Intell Prop. 351, 369 (2011), <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1005&context=njtip>.
- ⁶³ See A.T. Kearney, *Destination Latin America: A Near-Shore Alternative* 12 (2007), http://www.atkearney.com/images/global/pdf/Near-Shore_Latin_America_S.pdf (“Brazil hosts some of the world’s most competitive IT shops, and is becoming a world player in the ITO arena ... Brazil is in a good position to leverage its competitive advantage in ITO and further develop its BPO offerings.”); Stephanie Overby, *Outsourcing: Brazil Blossoms as IT Services Hub*, CIO.com (Sept. 8, 2010), http://www.cio.com/article/610635/Outsourcing_Brazil_Blossoms_as_IT_Services_Hub (noting that, according to industry estimates, “Brazil’s offshore outsourcing market hit \$1.4 billion in 2008, rising 75 percent in a single year”).
- ⁶⁴ Robert M. Sherwood, *Trade Secret Protection: Help for a Treacherous Journey*, 48 Washburn L.J. 67, 73-75 (2008).
- ⁶⁵ U.S. Int’l Trade Comm’n, *supra* note 34, at 4-13.
- ⁶⁶ Hearing Before the Subcomm. on Asia and the Pacific of the H. Comm. on Foreign Affairs, *supra* note 55, at 36.
- ⁶⁷ European Union Chamber of Commerce in China, *European Business in China Position Paper 2011/2012*, at 44 (2011), http://www.europeanchamber.com.cn/images/documents/pp_2011-2012/EN/PP%202011%20EN%20complete.pdf.
- ⁶⁸ U.S. Int’l Trade Comm’n, *supra* note 23, at 3-44.
- ⁶⁹ U.S. Int’l Trade Comm’n, *supra* note 34, at 4-14; see also Bai, *supra* note 62, at 362-63 (noting that “documentary evidence is practically the only form of evidence that carries significant weight in a Chinese court” and that “[i]t is advisable to have the recipient sign an acknowledgement of receiving access to the confidential information, in addition to executing a confidentiality agreement, prior to giving confidential information to a recipient”).
- ⁷⁰ Bai, *supra* note 62, at 362; U.S. Int’l Trade Comm’n, *supra* note 34, at 4-13.
- ⁷¹ See Baldia, *supra* note 59, at *233; Vinita Bali, *Data Privacy, Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?*, 21 Temp. Int’l & Comp. L.J. 103, 127-28 (2007).
- ⁷² Bali, *supra* note 71, at 128; Baldia, *supra* note 41, at *183-84.
- ⁷³ McAfee, *supra* note 8, at 15.
- ⁷⁴ Karen A. Magri, *International Aspects of Trade Secrets Law* 2 (1997), <http://www.myersbigel.com/library/articles/InternationalAspectsOfTradeSecret.pdf>.
- ⁷⁵ Keith Bradsher, *Hybrid in a Trade Squeeze*, N.Y. Times, Sept. 6, 2011, <http://www.nytimes.com/2011/09/06/business/global/gm-aims-the-volt-at-china-but-chinese-want-its-secrets.html>; Keith Bradsher, *G.M. Plans to Develop Electric Cars with China*, N.Y. Times, Sept. 21, 2011, <http://www.nytimes.com/2011/09/21/business/global/gm-plans-to-develop-electric-cars-with-chinese-automaker.html>.
- ⁷⁶ U.S. Int’l Trade Comm’n, *supra* note 23, at 3-22.
- ⁷⁷ Superseding Indictment, *United States v. Liew*, No. 3:11-cr-00573-JSW (N.D. Cal. Feb. 7, 2012); Exhibits to Opposition to Defendant Walter Liew’s Motion for Pretrial Release, *id.* (N.D. Cal. Jan. 31, 2012).
- ⁷⁸ Loretta Chao, *China Issued Record Number of Patents in 2009*, Wall St. J., Feb. 4, 2010.
- ⁷⁹ U.S. Int’l Trade Comm’n, *supra* note 23, at 3-43.
- ⁸⁰ *Id.*
- ⁸¹ ASIS International, *supra* note 3, at 41.
- ⁸² See Ponemon Institute, *State of Web Application Security: Executive Summary 1* (Feb. 2011), http://www.barracudanetworks.com/ns/downloads/White_Papers/Barracuda_Web_App_Firewall_WP_Cenzic_Exec_Summary.pdf.
- ⁸³ See ONCIX Report, *supra* note 5, at A-2.
- ⁸⁴ See Laurie S. Hane & Fraser Mendel, *Manufacturing Outsourcing and Offshoring to China*, 946 PLI/Pat 81, at *97 (2008) (“Due to the limited nature of the enforcement mechanisms to stop infringement, it is cheaper and more effective to implement proactive protective measures to mitigate the risk that the Service Provider misuses or discloses the Customer’s technology.”).
- ⁸⁵ Bai, *supra* note 62, at 365.
- ⁸⁶ Baldia, *supra* note 59, at *259.
- ⁸⁷ Jonathan Soble, *Japanese Rail Chief Hits at Beijing*, Fin. Times, Apr. 6, 2010.
- ⁸⁸ James T. Areddy, *In Toledo, the “Glass City,” New Label: Made in China*, Wall St. J., Aug. 29, 2010.
- ⁸⁹ See Dana Mattioli, *In China, Western Firms Keep Secrets Close*, Wall St. J., Aug. 30, 2010.
- ⁹⁰ *Id.*
- ⁹¹ *Id.*; see also Nat’l Intellectual Prop. Rights Coordination Ctr., *Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad* 53 (Nov. 2011) (warning that although manufacturing products in phases at different facilities “might protect against an insider who only sees one part of the process, sophisticated electronic spying may make such precautions ineffective”).
- ⁹² David Lazarus, *A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay*, S.F. Chron., Oct. 22, 2003, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/10/22/MNGC02FN8G1.DTL>; David Lazarus, *Pakistani Threatened UCSF to Get Paid, She Says*, S.F. Chron., Nov. 12, 2003, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/12/BUGI52VMQR1.DTL>.
- ⁹³ See Rubin, *supra* note 60, at 730 (noting that superseding public policy laws in the host jurisdiction, including laws relating to the validity of IP rights, may trump the applicable law selected by the parties in their contract).
- ⁹⁴ Baldia, *supra* note 45, at 515.
- ⁹⁵ Rubin, *supra* note 60, at 727.
- ⁹⁶ Mattioli, *supra* note 89.

CREATe.org

Center for Responsible Enterprise And Trade

ABOUT

FOCUS AREAS

NEWS & RESOURCES

“ In the 1990s, businesses used their supply chains to take on the problem of child labor in the developing world... Today, I'm encouraged that a new coalition of major companies is coming together to keep global supply chains free of pirated software and counterfeit goods. That gives innovators their rightful rewards, but it also creates American jobs.”

— U.S. Secretary of State, Hillary Clinton

About CREATe.org

CREATe.org is a nonprofit organization working with multinational corporations (MNCs) to foster innovation and economic prosperity by protecting intellectual property rights, fighting corruption, and driving responsible business practices in global supply chains and business networks.

We believe that by improving practices along global supply chains, multinational companies can help drive jobs, growth, and innovation—benefiting their own businesses, the global economy, and the communities where they operate. And by partnering with governments, nonprofits, think tanks, and associations, we hope to amplify the work of each.

To help achieve our shared goals, CREATe.org collaborates with these groups to develop and share practical tools and best practices, provide education, and advocate for the use of supply chains to strengthen a rules-based global system of commerce.

We are based in Washington, D.C., and our work is global.

For More Information

Please visit www.CREATe.org and follow us on Twitter at @CREATe_org. For more information, contact us via email at info@create.org. Our offices are located at 1401 Eye Street, NW, Suite 500, Washington, DC 20005.

CREATe Views

Intellectual Property and the U.S. Economy

At an event earlier today at the White House, the Department of Commerce released its new [Intellectual Property and the U.S. Economy](#) industries in E...

[More](#)

04/11/2012 [Add new comment](#)

Letter to the FTC on Intellectual Property

On Monday, April 2, a bipartisan group of senators and business leaders sent a letter to the FTC urging...



CREATE.org
Center *for* Responsible Enterprise And Trade