Hearing on

"Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

United States Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

May 13, 2014

Statement of Pamela Passman
President and CEO
Center for Responsible Enterprise & Trade
(CREATe.org)

Testimony of Pamela Passman
President and CEO of CREATe.org
Hearing on "Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"
May 13, 2014

Good afternoon Chairman Whitehouse, Ranking Member Graham, and members of the Committee. My name is Pamela Passman, and I am the CEO of the Center for Responsible Enterprise & Trade, also known as CREATe. I appreciate the opportunity to testify here today about an issue that is vital to the economy and job growth.

CREATe is a nonprofit dedicated to helping companies reduce corruption and intellectual property theft, including theft of trade secrets. We provide resources to companies large and small that help them assess their risks and develop strategies to protect their trade secrets and other IP assets, both within their own organizations and in their supply chains.

In today's integrated, global economy, information and knowledge are the new crown jewels. Companies that succeed in turning their knowledge and know-how into competitive advantage are the ones that will create new jobs and drive our nation's growth.

Increasingly, companies rely on trade secret laws to protect this knowledge. A trade secret can be as simple as a customer list, or as complex as the know-how to manufacture microchips. In our work at CREATe, it has become apparent that trade secrets are critical to innovation, and by extension to investment and competitiveness.

Yet the tremendous value of trade secrets also makes them prime targets for theft.

Calculating the extent and impact of trade secret theft is notoriously difficult. Many companies do not keep good track of their trade secrets, and those that do often do not know when their property has been stolen. Even when they are aware, companies often are hesitant to disclose thefts that have occurred, for both reputational and other reasons.

CREATe recently teamed up with PricewaterhouseCoopers to assess the economic impact of trade secret theft and devise a framework for companies to mitigate threats. A copy of the CREATe-PwC report is attached to my written testimony.

In the report, we used several proxies for estimating the value of trade secrets and the harms caused by trade secret theft. For instance, we looked at data on other key forms of illicit activity, such as fraud and corruption, copyright theft, and various black-market activities. Based on these proxies and other data, we estimated that trade secret theft costs on average 1 to 3 percent of GDP in the United States and other advanced economies.

Whatever the exact number, the problem of trade secret theft is massive and inflicts material damage on the U.S. and other economies. If we are to energize our economy by enabling innovative companies to protect their trade secrets, we need to focus on two key goals:

- First, we need to incentivize companies to take proactive measures and implement best practices to secure their trade secrets on the front end, both within their own organizations and in their supply chains.

- Second, we need a consistent, predictable and harmonized legal system to provide effective remedies when a trade secret theft has occurred.

I am therefore greatly encouraged to see the bipartisan interest in exploring better and more efficient ways to protect trade secrets. By providing attention to this issue, Congress can motivate companies to adopt more effective processes for protecting their own trade secrets; focus law enforcement attention; and put the United States on a path to having a harmonized legal system that will serve as a model around the world.

While there is an important role for governments in protecting trade secrets—and I applaud, Chairman Whitehouse and Ranking Member Graham, your focus on law enforcement—companies also need to take the lead in more effectively protecting trade secrets within their companies and in their supply chains.

Trade secret theft occurs through many vectors, and understanding these vectors can help businesses assess internal vulnerabilities that they can prioritize for fixing. Cybercrime is one clear avenue through which bad actors steal trade secrets, and I welcome this Committee's focus on cybercrime. Disgruntled employees and other malicious insiders, competitors, nation-states, hacktivists, and transnational criminal organizations, however, are other common avenues for trade secret theft. Companies need different tools and strategies to protect against each type of threat actor.

Businesses need to be particularly cognizant of risks that arise in their supply chains. The growth in recent years of extended global supply chains, comprising hundreds or even thousands of suppliers, has brought tremendous benefits and given many firms an enormous competitive edge. But companies using extended supply chains often must share confidential and highly valuable business information with their suppliers—many of which may be located in a different country with different laws and different corporate norms.

In the face of this reality, it is absolutely essential that companies implement effective strategies to protect trade secrets not just within their own four walls, but with their suppliers as well. In the CREATe-PwC report, we recommend a five-step approach for safeguarding trade secrets and mitigating potential threats:

- First, companies should identify and categorize their trade secrets throughout their organization.

- Second, they should conduct a risk assessment that identifies both the primary threat actors and potential vulnerabilities in the company's policies, procedures, and controls.

- Third, they should identify those trade secrets that have the greatest impact on the company's operations and business.

- Fourth, they should seek to assess the economic impact that would result from the theft of the most valuable trade secrets identified in step three.

- Fifth, companies should use the data collected in the first four steps to make informed decisions about how to allocate available resources and strengthen existing processes to most effectively increase the company's overall safety profile against trade secret theft.

CREATe recently completed a pilot program with more than 60 companies in countries around the world. We helped these companies assess their vulnerabilities to corruption and IP theft—including trade secret theft—and to implement procedures to mitigate these threats.

Based on that pilot program, we just launched "CREATe Leading Practices," a service designed to help companies improve and mature their management systems. On our website, companies can also find best practices and model policies. Employing these tools proactively can help companies protect their IP assets and remain competitive.

Unfortunately, no amount of protection can completely safeguard all trade secrets from theft. Companies also need a legal system that provides predictable enforcement and meaningful remedies against bad actors. A patchwork of different standards and enforcement mechanisms—whether domestically and internationally—makes protecting trade secrets significantly more difficult.

Recent high-profile criminal enforcement actions are encouraging, and a hearing like this, that highlights the value of trade secrets to the economy, will help prioritize criminal enforcement. Not all instances of trade secret theft are criminal, however, and law enforcement does not have the resources to investigate and prosecute all instances in any event. I am therefore encouraged by the efforts of Senators Coons and Hatch to create a harmonized system for owners of trade secrets to protect their property through a federal private remedy. Senator Flake's interest in theft that occurs overseas is also worth further study and discussion.

Our economy relies on the ability of companies to protect their trade secrets. Governments and companies both play a role in improving protection. In our view, companies would benefit from taking a more proactive role in assessing vulnerabilities and employing best practices to manage their risks. They also need an effective legal system through which to enforce their rights when their know-how has been misappropriated.

Thank you for holding this hearing and for giving me an opportunity to testify. I look forward to answering your questions.

# # # # #

Economic Impact of Trade Secret Theft:

A framework for companies to safeguard trade secrets and mitigate potential threats

February 2014

CREATE.org
Center *for* Responsible Enterprise And Trade

pwc

About this report

The Center for Responsible Enterprise And Trade (CREATe.org) has collaborated with PricewaterhouseCoopers LLP (PwC) to assess the economic impact of trade secret theft. Our effort has culminated in a report that focuses on four issues that are critical to understanding trade secret theft and how to improve companies' ability to protect their most valuable information:

- an estimate of trade secret theft across advanced industrial economies;
- a threat assessment focusing on what threat actors are most active in targeting trade secrets;
- an original framework for companies to assess the value of their own trade secrets; and
- a look forward 10-15 years in the future to consider what forces and drivers may make trade secrets more or less secure.

Governments, companies and individuals all play a role in improving trade secret protection. It is in every company's self-interest to improve trade secret protection and to use their leverage to encourage the companies they work with to do the same. Creating a shared sense of urgency can enable companies to dedicate resources to improve trade secret protection. Historically, such improvements have been viewed as a cost, not an investment. Our expectation is that this report will help companies shift that calculation of cost versus investment, enable companies to have a better understanding of who threatens their trade secrets and to provide new thinking and tools to help companies secure their trade secrets now and in the future.

Pamela Passman
President and CEO - CREATe.org
ppassman@create.org

Sanjay Subramanian
PwC | Principal
sanjay.subramanian@us.pwc.com

George Prokop
PwC | Managing Director
george.w.prokop@us.pwc.com

Table of contents

Introduction

In the private sector, trade secrets are fundamental building blocks that drive investment, innovation, and economic growth. The development of trade secrets also benefits the public good by enhancing economic security and stability.

For several years, the theft of trade secrets, often through cyber-enabled means, has been an important issue for the United States and other industrial economies. The deleterious impact of trade secret theft in both the private and public sectors all but ensures that this issue will remain a leading international priority requiring joint solutions to mitigate the ongoing threat and foster greater economic security throughout the international community.

The public sector has expressed a clear willingness to drive policy developments, foster international dialogue across governments, create public-private partnerships and prosecute actors responsible for trade secret theft. The private sector has an equally critical role to play in protecting trade secrets. The private sector's entrepreneurial spirit coupled with investor expectations will continue to drive companies to invest in research and development ("R&D") and develop new and innovative technologies. At the same time, companies must also invest in new measures to identify and mitigate their exposure to trade secret theft by fully understanding their own vulnerabilities and the threat actors targeting their enterprise.

Protecting trade secrets is critical for the continued prosperity and economic security of businesses around the world. In recent years, private and public sector organizations—universities, industry associations, think tanks, and government agencies—have studied this issue in depth. This paper addresses the broader economic issues referenced in other studies (e.g., national level estimates of trade secret theft); however, it primarily focuses on a framework for individual companies to:

1. Apply a risk-based approach to identify and prioritize their trade secret assets;
2. Analyze the direct and indirect economic losses attributable to a trade secret theft;
3. Understand the types of threat actors and how they may seek to inflict economic harm, as well as how those actors align with the company's vulnerabilities;
4. Develop new strategies to safeguard investment underpinning future trade secrets and mitigate the potential economic losses attributable to trade secret theft; and
5. Develop return on investment guidelines for implementing measures to improve trade secret protection internally and in the supply chain.

"The effects of [IP] theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses. American companies of all sizes are victimized. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries that can further expand the world economy and continue to raise the prosperity and quality of life for everyone. Unless current trends are reversed, there is a risk of stifling innovation, with adverse consequences for both developed and still developing countries."

– The Report of the Commission on the Theft of American Intellectual Property, 2013

The observations surrounding the assessment of the economic impact of trade secret theft and the accompanying company-level framework are grounded in an analysis of authoritative literature, our collective experience analyzing the economic impact of illicit activities, extensive open source research, our understanding of leading corporate governance and compliance protocols, and feedback garnered from workshops with leading private sector organizations. Our observations from these efforts include:

1. Estimates of trade secret theft range from one to three percent of the Gross Domestic Product ("GDP") of the United States and other advanced industrial economies.

Although numerous studies have attempted to analyze the losses attributable to trade secret theft, they have had mixed results, primarily due to concerns about the adequacy, completeness and reliability of private sector information. Beyond concerns about data, the analytic approaches of leading studies vary widely, resulting in disparate estimates of losses. Moreover, concerns about the potential adverse impact to a company's reputation in the market and ongoing relationships with customers limit the type of information companies are willing to disclose – either to industry partners or governments – about trade secret theft or internal vulnerabilities. Notwithstanding the challenges of developing national level estimates of trade secret theft, our analysis leverages multiple studies on illicit economic activity across the United States and advanced industrial nations as a proxy for the theft of trade secrets, resulting in an estimate of 1 to 3 percent of U.S. GDP.

2. The national level estimate of trade secret theft is important as a guide to policy creation, industry awareness and advocacy, but is less relevant to individual companies.

At the company level, firms can gain tangible benefits from understanding the relative value of their trade secrets. Analyzing the portfolio of trade secrets that a company keeps and understanding the potential direct and indirect costs (e.g., lost revenue, disruption of business, tarnished reputation) that their theft would inflict is a critical step in a broader company process of prioritizing limited resources to protect trade secrets. In doing so, a company can develop viable estimates on the return on investment it would get from improving trade secret protection, as the probability and severity of a potential breach can be factored into these calculations.

"A consensus among economists has emerged that trade secrets play an important role in protecting the returns to innovation and that trade secret protection is an integral and important part of the overall system of protection available to EU firms to protect their intangible assets, like patents and copyrights."

– European Commission Study on Trade Secrets and Confidential Business Information in the Internal Market, April 2013

3. A company-level approach to estimating losses attributable to trade secret theft will drive more reliable national level results, but companies can do more than serve as the subjects of anecdotes.

In many instances, companies are referenced in anecdotes about trade secret theft, but refrain from proactive contributions to a broader public dialogue on this issue due to aforementioned concerns about adverse press, stakeholder relationships, market considerations, and/or regulatory exposure. Reticence may also exist because most companies do not yet have standard procedures to consistently or systematically identify or prioritize their trade secret portfolio, let alone consistent means to assess the economic impact of the loss of trade secrets. Better informed dialogue among the private sector, coupled with a framework for considering these complex issues at the company level, may yield substantial long-term benefits to both public and private sector stakeholders.

4. Increasing company-level awareness of the internal and external threat environment facilitates enhanced protection of trade secrets, an improvement in the quality of the national level estimate of trade secret theft over time, and the potential for a long-term reduction in losses.

Threat actors come in many forms. Malicious insiders, competitors, nation states, hacktivists and transnational organized crime are only a few examples. Gaining an understanding about who those actors are, their motivations and typologies, and their target selection process can enhance the private sector's understanding of how these actors may seek to exploit a company's vulnerabilities. Similarly, understanding the means by which they go about stealing trade secrets can highlight internal vulnerabilities that companies can prioritize for fixing. For example, while the current focus may be on cyber-enabled means of stealing trade secrets, many threat actors still rely on physical means such as recruitment of insiders and placement of agents within companies for purposes of stealing critical data. Keeping current on trends related to threat actors and their methods helps companies take meaningful steps to better safeguard their assets and mitigate such threats.

5. Modeling future scenarios highlights the drivers influencing trends in trade secret theft and provides insights that enable companies to create long-term strategies to protect trade secrets.

By looking forward and considering how threats against trade secrets and other forms of intellectual property may evolve over the next 10-15 years, companies can increase their awareness of how these drivers and factors, if not properly aligned, could make it harder to protect trade secrets. These scenarios can enable companies to visualize and plan for a more secure future for their trade secrets and, at the same time, enhance their ability to make investment decisions today.

6. Management will be better able to formulate and implement new strategies to safeguard investments and mitigate threat if armed with a greater understanding of current and future trends, threat actors seeking to engage in illicit activity, companies' own trade secret portfolios and organizational vulnerabilities.

To maintain competitive advantage in the global marketplace, companies will continue to make significant investments to develop new products and services, the protection of which will be critical. Coupled with the consistent threat of a trade secret theft event and the deleterious impact it can have, management can justify the need to increase company, supply chain and business partner awareness of the threats and trends, and implement protective measures to safeguard these valuable investments. These protective measures can include improved IP protection management systems and improved technology.

Scope, Approach and Limitations

CREATe.org and PwC collaborated to (i) analyze the economic impact of trade secret theft in advanced industrial economies, and (ii) develop a company-level framework to aid the private sector in its efforts to address this important issue. This study furthers CREATe.org's mission as a non-profit organization dedicated to helping companies and their suppliers and business partners reduce counterfeiting, piracy, trade secret theft and corruption.

Definition: Trade Secret

For the purposes of this report, we use the definition of a "trade secret" set forth in the U.S. Economic Espionage Act ("EEA"). It is similar to the definition of trade secrets under the Uniform Trade Secrets Act that has been enacted by 47 U.S. states and several U.S. territories, consistent with Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) and Article 2 of the Japanese Unfair Competition Prevention Act. Under the EEA, trade secrets are:

…all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, analyses, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if - (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public…[2]

Approach

This study is based in part on CREATe.org's efforts in the market to heighten trade secret awareness, increase and improve collaboration amongst companies and between the private and public sectors, and assist companies in fostering a better understanding of the tools companies have at their disposal to categorize, document, and protect their trade secrets through improved management systems and utilization of technology.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft. It estimates the losses attributable to trade secret theft across advanced industrial economies using a proxy approach that measures other forms of illicit economic activity. However, recognizing that this approach only serves as an estimate, we collectively developed a framework to assess the economic impact of a trade secret theft event at a company level by applying more traditional economic analyses and techniques. The framework relies on dual methodologies including: (a) a direct method to estimate the lost future revenue and profitability associated with the theft of a trade secret, and (b) an indirect method evaluating the more intangible adverse impacts of such an event, as measured through various non-financial performance indicators. Our approach incorporates inputs on threat actors, probability and severity of incidents, organizational protections and vulnerabilities, and future trends analysis that companies should consider. These inputs drive the economic impact of a trade secret theft event and are important elements that companies should factor into their assessment of how to protect their trade secrets. In this context, the study may be viewed as a guide for individual companies, and as a path forward to a future national level estimate.

The study is broken into the following phases:

1. An estimate of trade secret theft across advanced industrial economies;
2. An analysis of the threat actors who are actively engaged in trade secret theft;
3. A framework enabling companies to conduct their own internal evaluations and inventories of existing trade secrets, assess their vulnerabilities to loss, estimate the economic impact of a trade secret theft event, and provide new insights on how to protect these assets; and
4. An outlook for the future of trade secret theft using the results of a futures modeling exercise—drawing from workshops with private sector participants—that present scenarios for future developments and concerns.

Taken together, these sections represent a broad approach to evaluating the aggregate impact of trade secret theft by starting at the company level, and giving companies the tools needed to effectively manage and protect their trade secrets. This practical approach recognizes that fostering greater activity and awareness of this issue among individual companies may produce significant advancements on this challenge.

Limitations

The framework is an approach we collectively developed based on our experience and interaction with numerous companies and organizations facing trade secret theft. It is meant to serve as a guide for companies to document and analyze their trade secrets so they may apply their resources in a cost effective and efficient manner. Application of the framework will not necessarily prevent a trade secret theft event, but may enable companies to better identify and mitigate threats as they arise due to greater understanding of the threat landscape and their internal vulnerabilities, and to be more strategic in allocating resources to protect their trade secrets.

Our outlook section in which we discuss the results of our futures modeling exercise addresses how trade secret theft issues may play out globally, not only in the U.S. The scenarios should not be read as predictions, but rather as a survey of how trends could evolve under certain future conditions. They were created using four drivers in different combinations. These drivers are only four among many that will likely play a critical role in trade secret protection in the years ahead.

Our approach reflects the significant and growing body of literature on the topic of trade secret theft.

Estimate of Trade Secret Theft

Estimating the value of trade secrets at a national or global level presents significant challenges. In this section we will address these challenges and present an approach to estimating the economic impact of trade secret theft.

Obstacles to Estimating Trade Secret Value

Trade secrets, intellectual property ("IP"), and other intangible assets represent a large and growing share of U.S. and global economic activity. The growing number of patents issued by the U.S. Patent and Trademark Office illustrates the essential role intangible assets play in supporting a dynamic global economy. From 1990 to 2010, the pace of innovation in the private sector spurred the growth of intellectual property and the number of patents issued in the U.S. increased by 40.6 percent, jumping from 99,200 patents issued in 1990 to 244,300 in 2010. Notwithstanding the central and powerful role that IP plays in the global economy, there is no consensus on the exact value of trade secrets or how to estimate such a figure.

Numerous academic, industry, non-profit and government reports highlight the challenges in estimating the overall value of trade secrets and the economic impact of those that are stolen. For example, a May 2013 study by the Commission on the Theft of American Intellectual Property ("Commission")—an independent and bipartisan group chaired by Admiral Dennis Blair and Ambassador Jon Huntsman—assessed various dimensions of international IP theft and its impact on American businesses. The Commission concluded that the exact value of IP theft was "unknowable," but added that existing assessments of loss have underestimated the impact of IP and trade secret theft. The Commission offered three explanations for why trade secret value was so difficult to measure:

1. Loss is measured in different ways in different sectors;

2. Companies do not often report their losses and are not incentivized to do so out of fear of impact on stock prices and marketplace reputation; and

3. Surveys are often used to measure loss and they are not sufficiently dependable to offer details on such a vast problem. [5]

In another example, a 2010 Government Accountability Office ("GAO") study analyzed the economic effects of counterfeit and pirated goods and found that "it was not feasible to develop our own estimates [of the total value of counterfeit or pirated goods] or attempt to quantify the economic impact of counterfeiting and piracy on the U.S. economy."[6] Noting the lack of data as a primary challenge to quantifying the economic impacts of counterfeiting intellectual property and goods, the GAO concluded that "neither governments nor industry were able to provide solid assessments of their respective situations" suggesting the need for individual companies to evaluate the worth of their own trade secrets.[7]

After reviewing these and other studies, as well as conducting an independent analysis of trade secret theft, we noted additional considerations that impede estimation of the value of trade secrets:

- The volume of data required to construct an accurate assessment that withstands scrutiny is significant, and would face substantial legal and analytic challenges;
- Some companies are simply unaware that their trade secrets have been stolen, while other companies are reluctant to report such losses to third parties due to concerns about reputational or financial repercussions; and
- Such an assessment would by its nature be somewhat fleeting. As soon as such a figure was agreed to, the value of the trade secrets at the heart of the analysis would have already begun to shift across individual companies or industry sectors.

Purpose of Utilizing Proxies to Estimate Trade Secret Theft

Given the inherent methodological challenges of estimating the value of trade secrets at a national or global level, a proxy approach to estimating the value

of trade secrets can be useful and provides interesting insights. Seemingly unrelated activities—such as research and development spending, occupational fraud, and tax evasion—share important traits with trade secrets, and provide insightful context that enables reasonable estimation of the economic impact of trade secret theft.

Proxy for the Value of Trade Secret Theft: Research and Development

A core proxy for the value of trade secrets involves private sector expenditures on R&D. There are numerous valuable trade secrets that are not related to R&D (such as customer lists, sales data, marketing information, etc.) but R&D represents investment in new ideas, methods, tools and techniques—each of which are critical elements of many trade secrets. Since the early 1980s, R&D expenditures in the United States have exceeded 2.5 percent of GDP; U.S. Government figures report the figure as $414 billion or 2.7 percent of GDP in 2011.[8]

Global R&D investment trends are similar to U.S. trends. Battelle and *Research & Development Magazine's* 2014 "Global R&D Funding Forecast" examine global R&D for the top 40 world economies (ranked by nominal GDP) and levels of actual and projected spending. As illustrated in Figure 1, they conclude that R&D for the top 40 national GDPs averaged nearly 2 percent in the last three years and are forecast to maintain this level in 2014. Over the last three years, R&D as a percentage of global GDP has also remained steady at 1.8 percent.[9]

Current R&D spending, of course, generates other forms of trade secrets, and represents only a fraction of the economic value generated by R&D. Researchers have estimated that $1.00 of spending on R&D produces about $2.90 in other economic activity during the same year and between $16.00 and $69.00 over the next 10 years.[10,11] On this basis, the value of trade secrets in the marketplace represents a significantly greater component of GDP than illustrated by R&D spending alone.

Proxy for the Estimate of Trade Secret Theft: Illicit Economic Activity

Proxies involving illicit economic activity also clarify the potential impact of trade secrets theft. Such measures capture economic behavior that may inflict harm on the global economy and, like trade secret theft, are under-reported and difficult to measure. Also, in a manner similar to their approach to trade secrets, certain threat actors will target these areas for a variety of economic (e.g., market share, profitability) and non-economic (e.g., increase influence, advance social causes) reasons:

Figure 1: R&D as a percentage of GDP

	2011	2012	2013	2014
U.S.	2.7%	2.8%	2.8%	2.8%
China	1.5%	1.8%	1.9%	2.0%
Japan	3.5%	3.4%	3.4%	3.4%
South Africa	1.0%	1.0%	1.0%	1.0%
Germany	2.9%	2.8%	2.8%	2.9%
Australia	2.3%	2.3%	2.3%	2.3%
UK	1.8%	1.8%	1.8%	1.8%
Russia	1.5%	1.5%	1.5%	1.5%
Qatar	2.8%	2.8%	2.8%	2.7%
Brazil	1.2%	1.3%	1.3%	1.3%
Average (Top 40)**	2.0%	2.0%	2.0%	2.0%
Rest of World	0.4%	0.4%	0.4%	0.4%
Global Average	1.8%	1.8%	1.8%	1.8%

*2014 figures are projected

**Top 40 world economies by GDP

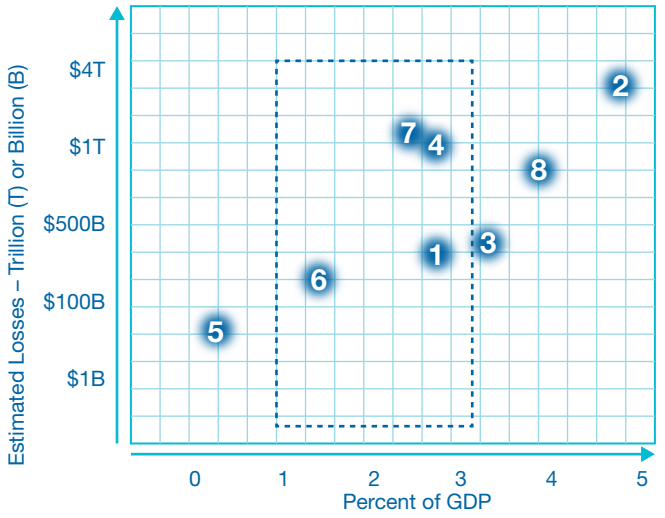
Sources: 2013 & 2014 Global R&D Funding Forecase, Battelle and R&D Magazine.
Sub-Sources: IMF, World Bank, CIA World Fact Book

- ***Occupational Fraud:*** Companies worldwide lose as much as $3.5 trillion, or 5 percent of global GDP, due to occupational fraud and abuse, according to a 2012 report based on the analysis of nearly 1,400 fraud cases by the Association of Certified Fraud Examiners ("ACFE").[12] Facing a similar set of threat actors as trade secret theft—namely malicious insiders with unparalleled access to systems, these perpetrators make measuring fraud and abuse difficult.
- ***U.S. Tax Evasion:*** In a 2013 study the U.S. Internal Revenue Service ("IRS") estimates the tax gap—the difference between what taxes are owed and what taxes are collected—to be approximately $450 billion, or 3.25 percent of U.S. GDP. The IRS assesses that the tax gap is a result of nonfiling, underreporting and underpayment—and that it can be challenging to determine what activity is illegal.[13]

- ***Corruption:*** Another significant issue that often defies exact accounting is global corruption, defined traditionally as the abuse of public office for private gain. Like trade secret theft, corruption poses a unique threat to both the public and private sector by eroding confidence in the rule of law as well as undermining competition. A study sponsored by the World Bank estimates the annual cost of such activities as some $1 trillion, or 2.9 percent of global GDP in 2005.[14]
- ***Copyright Infringement and Software Piracy:*** Copyright theft, copyright infringement and software piracy are widely recognized challenges for advanced industrial economies. A 2012 Business Software Alliance ("BSA") report noted, for example, that some 42 percent of global personal computer users employ pirated software, reaching a commercial value of $64.3 billion in 2011, or 0.1 percent of global GDP. A diverse group of threat actors targeting trade secrets may also be interested in pirating software. Criminal groups are known to pirate software strictly for profit, while hacktivists may attempt to damage the reputation of software companies by creating pirated software that damages systems and users, resulting in negative publicity for the software's true originators.[15]
- ***Narcotics Trafficking:*** Like the theft of trade secrets, the trafficking of narcotics inflicts a variety of economic costs, including workers' lost productivity, medical treatment, and the administration of justice. In a 2011 study of the impact of illicit drug use in the United States, the U.S. Department of Justice estimated the cost in 2007 to be as high as $193 billion, or about 1.4 percent of U.S. GDP in 2007.[16]
- ***Black Market Activities:*** At the global level, the value of black-market activities is estimated at $1.8 trillion—approximately 2.5 percent of global GDP—according to information compiled on the crowd-sourced database Havocscope. This estimate includes a diverse range of activities that are challenging to quantify: counterfeiting of products like aircraft parts, food, weapons, cosmetics, watches, and clothing; trade in endangered wildlife; art theft; illegal gambling; bootlegging of tobacco and alcohol; and human trafficking.[17]
- ***Illicit Financial Flows:*** The illegal movement of money from developing countries to financial institutions in developed states is, in some ways, a mirror image of the theft of trade secrets, which typically involves the illicit transfer of sensitive information in the opposite direction. In a 2013 study of 55 developing countries funded by the Ford Foundation, economists' estimated that illicit financial outflows—most in the form of mis-invoicing of trade—amounted to $947 billion in 2011, some 3.7 percent of these countries' combined GDP.[18]

Taken together, these proxy measures provide context for trade secret theft as yet another form of illicit economic activity and corroborate its significant impact on national economies. As illustrated in Figure 2, most of these measures are clustered between 1 and 3 percent of GDP. While it is difficult to accurately measure economic losses attributable to trade secret theft at a national or industry level, this proxy approach provides a reasonable estimate of the economic impact of trade secret theft given the similarities between trade secret theft and other forms of illicit activity.

Figure 2: Proxies for Estimate of Trade Secret Theft



Analysis of Threat Actors Engaged in Trade Secret Theft

Numerous actors—foreign intelligence services, competitors, transnational criminal organizations, hacktivists and malicious insiders—target and steal companies' trade secrets for various reasons. Social engineering schemes such as tailored spear-phishing campaigns that implant malware to steal trade secrets, or duping employees into revealing sensitive corporate information, exemplify the means by which these actors engage in trade secret theft. Constantly evolving technologies in smart phones, laptops, and tablets that employees use for work provide additional means for threat actors to access a company's secrets. Threat actors' motivations are equally diverse. Some seek personal financial gain, while others hope to advance national interests or political and social causes.

Many threat actors are known to target and steal trade secrets. The threat actors profiled in this section were selected using a risk-based methodology that considered several factors:

- A well-documented track record of attacking multinational companies;
- Intent to misappropriate companies' trade secrets and critical data;
- The capability, as demonstrated by past attacks and by U.S. and other government reporting, to target companies' trade secrets for their own profit or to advance another country's interests;
- Intent to attack companies and institutions that are rich in trade secrets and other valuable corporate data;
- Consistent focus on specific industries and sectors—information and communications technology, aerospace & defense, marine systems, clean technologies, advanced materials and manufacturing, healthcare and pharmaceuticals, agricultural technology, energy and natural resources—consistent with the 2011 Economic Espionage Report;[19] and
- Demonstrated impact on companies due to the theft of trade secrets.

The more effectively that companies can understand these actors and their respective typologies, the better equipped they will be to manage their trade secret portfolios and apply appropriate protection measures that are calibrated to the economic value of specific trade secrets, the type of actor and the type of threat. Companies able to understand who may seek to steal their trade secrets are better able to view those secrets through the lens of a threat actor, and therefore apply appropriate resources to enhance their security.

Nation States

Nation states have unmatched resources and capabilities for stealing trade secrets, and usually want to acquire foreign trade secrets to strengthen their existing military capabilities and bolster national champion companies in the global marketplace.[20] Many foreign intelligence and security services attempt to acquire trade secrets and sensitive economic information on behalf of their governments, commonly using covert means. Nation states may also use other national agencies, regulatory powers, or state-supported organizations. Some even publicly claim this is part of their missions. For example, the decree establishing Russia's Foreign Intelligence Service assigns it responsibility for "protecting the country's economic development and scientific progress."[21] Other examples of nation state actors trying to collect trade secrets from companies include:

- The head of a German satellite company told U.S. diplomats in 2009 that France represented a greater danger to his country's IP than any other country.[22]
- In 2011, a former employee of a major American chemical company pled guilty to committing economic espionage that benefitted elements of the Chinese government.[23]
- South Korean intelligence officers have been found trying to obtain economic secrets from Australian officials in 2013, according to multiple reports.[24]

Malicious Insiders

Current and former employees, third parties acting as consultants or lawyers, and suppliers often have unique access to corporate trade secrets and other information that, if released, could inflict significant harm on a company. Respondents to PwC's *2013 U.S. State of Cybercrime Survey* identified current and former employees as one of the greatest cyber security threats they faced.[25] Insiders' knowledge of companies' systems, where and how information is stored, and specific details on the production or use of trade secrets makes insiders a uniquely dangerous threat. The threat from malicious insiders is all the greater because insiders often cooperate with other threat actors who can provide money, other resources, or ideological motivation. Examples of the cost insiders inflict on companies with high value trade secrets include:

- In 2012, a former employee of a North American automotive company and the employee's spouse were found guilty of stealing trade secrets related to hybrid vehicle technology worth $40 million. The couple intended to sell the information to a Chinese competitor.[26]
- An employee of a large U.S. futures exchange company pleaded guilty in late 2012 to stealing more than 10,000 files containing source code for a proprietary electronic trading platform. Prosecutors estimated the value of these trade secrets between $50 and $100 million. The employee said he and two business partners had planned to use this source code to develop their own company.[27]
- In 2011, a former employee of an automotive company was sentenced to 70 months in prison for copying some 4,000 documents on the design of engine-transmission and electric power supply systems. The employee intended to take these documents to a new job with the China branch of another North American company.[28]

"Ultimately, cybercrime is not strictly speaking a technology problem. It is a strategy problem, a human problem and a process problem."

– PwC Global Economic Crime Survey, 2014

Cultural and technological factors may heighten the insider threat in coming years. A study noted that the nature of U.S. employees' loyalty to their employers is changing because of the much higher rate of lifetime job changes in the 21st century, as compared to the mid-20th century. At the same time, growing numbers of people with highly sought-after technical skills often cross international borders for work, which means more employees with potentially competing sources of loyalty. Additionally, the growing prevalence of "bring your own device" policies and the ease and speed with which employees can move data across multiple programs and applications hampers security and monitoring efforts. These factors could increase the population of malicious insiders with increased access and a diminished sense of obligation to their employer – factors that may increase the risk that they will use their status to expose trade secrets and other sensitive corporate data.[29]

Competitors

Competitors can target companies' trade secrets independently or with assistance from national governments; cases involving competitors stealing trade secrets represent a large portion of U.S. Department of Justice trade secret theft cases. From these cases we see that competitors can use several methods, including recruiting employees of the targeted company who are disgruntled or have personal ties to the competitor's home country to steal trade secrets or sensitive corporate data. Other methods include bribery, extortion, or the promise of a new job.

Even when acting independently of national governments, corporate competitors often have the resources to exercise state-like power. The repeated use of insiders and corporate spies to access critical and sensitive data is illustrated by recent trade secret theft cases involving competitors:

- A sting set up by U.S. law enforcement uncovered attempts to bribe an undercover agent posing as a corrupt lab technician of a major U.S. pharmaceutical company that had recently spent millions to develop formulas for a new drug. The indictment noted that the successful theft of the formula could have resulted in billions of dollars of losses for the company.[30]
- In a case involving Asian and North American chemicals companies, the Asian firm is alleged to have hired current and former employees of the North American company as consultants in order to have them reveal confidential and proprietary information. This enabled the Asian company to replicate a proprietary manufacturing process and earn at least $225 million in proceeds from the theft of the trade secrets.[31]

Transnational Organized Crime ("TOC")

Transnational Organized Crime groups have successfully attacked numerous corporate information technology networks to access payment systems and steal personally identifiable information, personal health information, and payment card information, inflicting massive financial damage on their targets.[32] As TOC groups expand their activities beyond long-standing activities such as gambling or racketeering, many well-established groups are increasingly leveraging the Internet for all manner of cybercrimes.[33] In this role they are serving as facilitators that enable other threat actors, such as unscrupulous competitors or intelligence services, as they attempt to steal trade secrets.[34]

A computer security company recently noted the emergence of "cybercrime-as-a-service,"[35] and TOC groups often work with other established cyber criminals, purchasing information they have stolen via electronic means for the purposes of furthering their own traditional organized crime agendas.[36] In 2013, the Director of National Intelligence warned that cybercriminals could "enable access to critical infrastructure systems or get into the hands of state and non-state actors." This dimension of cybercrime is increasing the availability of hacking tools that can be used to steal trade secrets, potentially allowing threat actors to easily rent or buy sensitive corporate or other information.[37]

Hacktivists

Hacktivists seek to expose sensitive corporate information—potentially including trade secrets—to advance political or social ends. These groups have used cyber intrusion skills and data gleaned from disgruntled insiders to obtain and publish Personally Identifiable Information (PII) and sensitive business information of key executives, employees, and business partners. As with TOC groups, hacktivists have the technical knowledge and capabilities to steal trade secrets, and they could partner with other threat actors for ideological or financial reasons.

Greater awareness of the threat actors attempting to steal trade secrets, their capabilities, and typologies can position company management to understand their vulnerabilities to theft by these actors and to formulate and implement strategies to mitigate these threats. The following section incorporates this understanding and lays out a scalable framework that companies can use to (i) assess the company-level economic impact attributable to trade secrets theft, and (ii) enhance their ability to safeguard investments and mitigate future losses.

A Framework for Individual Companies to Safeguard Trade Secrets and Mitigate Potential Threats

The growing threat of trade secret theft and the adverse economic implications it creates for the private sector require companies to be increasingly proactive in managing this threat to achieve their strategic, operational and financial goals.

In response, CREATe.org and PwC developed a multi-level framework for private sector organizations to analyze their trade secret portfolios. The framework provides a platform to identify and categorize trade secrets leading to an analysis that yields insights into threat actors seeking to induce economic harm, vulnerabilities in companies' existing control structure and a model to assess losses attributable to the theft of a trade secret. Collectively, this framework provides companies with a means to identify potential gaps or exposures in their trade secret protection strategies and ideas to further their ability to safeguard their investment and mitigate future losses. It also provides critical information that enables companies to better understand the return on investment of improved trade secret protection and how to strategically allocate resources. An illustration of the framework is presented in Figure 3.

This section of the paper describes the activities and key points for management's consideration for each level of the framework. As a reference to illustrate the framework's application, each level provides further explanatory guidance on how *ABC Widgets, Inc. ("ABC")* proceeds through the framework. *In our example, ABC is a large, global, publicly-traded, U.S.-based alternative energy company, with a widely-dispersed third-party supply chain and aggressive plans to expand into new markets.*

In our scenario, ABC's executives and board members are becoming increasingly aware of advanced threats to its intellectual property and, in particular, its trade secrets based on recent media reports about attacks against ABC's competitors. At a quarterly board meeting, ABC's directors question management about its plans to mitigate such threats. Reluctantly, ABC's management acknowledges that they have not yet thoroughly identified its portfolio of trade secrets, nor implemented a trade secret protection management system, and will quickly endeavor to analyze these issues with the goal to seek opportunities to strengthen the company's ability to mitigate such threats.

Figure 3: A framework for assessing the business impact of trade secret loss

Level 1: Identify Trade Secrets

Our collective experiences indicate that many companies fail to effectively manage their trade secret portfolios for multiple reasons, including a lack of consensus on what assets actually constitute the portfolio. Some companies' reticence may also stem from their interpretation of "reasonable measures [are] taken to protect [trade secrets] the information"[38]—mistakenly deducing that any specific documentation of trade secrets potentially creates exposure for the company in the event of a breach. Reasons for this could include concerns about incomplete documentation, lack of follow through, or other such errors or inconsistent practices, but the net result is the fear that courts will find the company has not met the reasonable measures standard. Such companies may prefer taking a general, blanket approach to security and confidentiality that could apply to any information the company may later identify as a trade secret. Our view is that individual companies must weigh the benefits of this thorough approach against the risks, costs, and the company's ability to abide by the basic tenets of the framework, while also considering the risks inherent in not closely protecting the company's most sensitive trade secrets.

This first level of the framework takes the organization through the basic, yet critical step of identifying and categorizing its trade secrets. To best protect those trade secrets whose theft would cause the most harm, companies should first document, locate and inventory their trade secrets. This first step gathers key stakeholders—senior executives, business unit leaders, corporate functional leaders—to inventory the trade secrets maintained by the company. Ultimately, forming a cross-functional team with senior management support is critical to this step and those that follow. Discussion and debate of what constitutes a trade secret for the company is encouraged, as stakeholders should emerge from Level 1 with a broad consensus of not only the definition of a trade secret for their company, but also a list of the company's trade secrets aggregated into categories such as those summarized in Figure 4.

In response to the Board of Directors' queries, ABC embarks on a process to identify its trade secrets. ABC's Compliance Counsel is designated by ABC's Executive Leadership Team to lead the effort. Having recently attended a conference on intellectual property matters, she too started to become aware of the emerging threats to ABC's trade secrets.

Figure 4: Trade Secret Categories

Category of Trade Secrets	Examples
Product Information	New hardware designs; adaptations/updates of existing products
Research & Development	Long-term R&D; basic or applied research; geology R&D
Critical & Unique Business Processes	Inventory/distribution; manufacturing processes; business model based on application of processes
Sensitive Business Information	M&A prospects/plans; market research/studies; customer list/information; information on key suppliers/business partners; expansion plans; corporate strategy
IT Systems and Applications	Novel application of IT that could create new markets; system architecture designs; source code; algorithms

She researches applicable laws, regulations and standards governing trade secrets. She also studies ABC's existing policies and determines that ABC does not maintain a central repository or conduct standardized procedures to manage their portfolio of trade secrets. Recognizing that much work needs to be done, she initiates a working session with a cross-functional team of ABC's senior executives, business unit leaders and corporate functional leaders to inventory the company's existing trade secrets across the categories highlighted in Figure 4.

Before the working session, ABC's Compliance Counsel distributes a working definition of a trade secret and encourages participants to engage in a lively debate. Participants arrive at the working session with their lists, which they present, discuss, and compile into a master list that aligns with ABC's views about what constitutes a trade secret. The meeting results in a categorized list of valuable trade secrets reflecting critical elements of ABC's business model.

Following the working session, the Chief Information Security Officer ("CISO") tasks staff to leverage technology solutions to search across the organization for the assets identified during the working session. Using tools that search based on keywords and other identifiers, trade secrets from the master list are found on various servers, in files with non-relevant file names, and on shared-file sites created for reasons unrelated to the trade secret itself. The results for the location of each trade secret found are noted on the master list, to be incorporated later into the vulnerability assessment. The CISO will also work with other business leaders to find trade secrets—which could may exist off the network, in hand-written notes, prototypes, etc.—to ensure that as many trade secrets as possible are located regardless of their presence on IT systems.

By completing Level 1, companies have an agreed-upon list of a company's critical trade secrets—a critical first step in this framework. Many of the trade secrets are also located across the organization, which will contribute to understanding how vulnerable they are to theft. However, as organizations continue to design new technologies or engage in new ventures, they will continue to develop and/or acquire new trade secrets. Therefore, management must establish procedures to continuously refresh this inventory on a periodic basis to facilitate its completeness.

Level 2: Threat Actor and Vulnerability Assessment

A risk assessment focused on threats and vulnerabilities forms a critical step in the framework. As noted earlier, threat actors take many different forms, each of which poses a significant threat to a company's intellectual property. Analysis of existing trade secret protection management systems—the compliance and security program policies, procedures and internal controls—enable management to identify vulnerabilities in its current protocols that may create unnecessary risk and exposure for the company. Evaluating the maturity of the overall trade secret protection program and the specific processes is an effective way to understand the vulnerabilities.

2.1: Threat Actor Assessment

Operating in today's global marketplace exposes companies to unique and varied threat actors. As such, management must understand the scope of the company's operating environment (e.g., office locations, sales/marketplace footprint, supply chain, product/service mix, key personnel, and growth strategies) in context of the potential threat actors seeking to engage in illicit activity to adversely impact the company. Assessing the risk posed by individual threat actors within this construct, the probability that they will attempt to steal a company's trade secrets, and the severity of such an event, is critical to determining which trade secrets merit the highest level of protection and enables management to implement more effective protective measures.

As part of its threat assessment, ABC's Compliance Counsel analyzes the company's operating environment, including markets in which the company operates, major customers, significant supply chain and business partners, key executives, employees' access to trade secrets, existing products/services, and designs for new product launches and/or mergers and acquisitions (M&A) activity.

In this context, ABC analyzes the various threat actors that may impact its operating environment and the risk they pose, paying particular attention to the probability and potential severity of a breach. With ABC's leading market position in the industry, it suspects certain threat actors (i.e., malicious insiders, nation states) warrant closer attention and monitoring due to recent data breaches resulting in the theft of intellectual property at ABC's competitors in locations where ABC also has production facilities. Using Figure 5 as a general guide, ABC researches recent incidents to understand the potential threat actors targeting the company and the likelihood of a malicious action from them.

Figure 5: Potential Threat Actors' Goals, Tools, Vectors and Targets

Threat actor	Goals	Tools and vectors	Trade secrets that could be targeted in your firm
Nation states	• Technology to support military capabilities • Strengthen "national champion" companies	• Foreign intelligence and security services • Cyber vector • Human intelligence operations • Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects. • Co-opted entities such as state-owned enterprises	• Items with direct military applications, such as aerospace technologies • "Dual-use" products, such as IT technologies and navigational systems, with both civilian and military applications
Malicious Insiders	• Competitive advantage • Financial gain • Advance national goals	• Access to sensitive company information • Manipulation of weak protections, lack of oversight over trade secrets • Can access trade secrets on electronic/IT systems or that are hardcopy only	• Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans • "Dual-use" products • Sensitive data on customers or suppliers
Competitors	• Competitive advantage	• Cyber vector • Technical tools such as electronic eavesdropping, acoustic cryptanalysis, video surveillance and wiretaps • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Data that enables your firm to differentiate its services and products in your sector, such as source code or marketing plans
Transnational Organized Crime	Financial gain • PII, other financial data • Cybercrime as a service sold to others	• Cyber vector • Some TOC groups willing to undertake physical attacks against company leadership, personnel and facilities • Use of insiders • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Any trade secret perceived as vulnerable to exploitation
Hacktivists	• Advance political or social goals by exposing sensitive corporate information	• Cyber vector • Exploitation of open source information concerning companies' executives, vulnerabilities or projects.	• Sensitive data on customers or suppliers • Production/distribution technologies

2.2: Vulnerability and Protection Analysis

Threat actors often seek to exploit vulnerabilities in an organization's governance, financial, technology, operational or compliance architecture leading to opportunities for illicit behavior that create economic harm to the company. Accordingly, companies must proactively identify potential internal vulnerabilities in their policies, procedures and controls, as well as their reliance on suppliers and other business partners, and take steps to mitigate any exposure resulting from these weaknesses. These vulnerabilities can range from a lack of training on information security to employees using software without routinely checking for updates, to a highly valuable trade secret stored on an unsecured server with broad access within the company, to a lack of awareness among employees of where trade secrets are kept. Trade secrets can be gauged on a continuum from "fully protected" to "unprotected," and a narrative documenting the type and strength of protection, as well as the remaining vulnerabilities, can be attached to each trade secret. A critical component of the vulnerability assessment is to assess the maturity of the trade secret protection management system.

For each trade secret identified and located during the Level 1 inventory analysis, ABC's Compliance Counsel collaborates with senior executives and corporate functional leaders (e.g., CFO, CIO, CSO, CISO) to review where the information is stored and catalogs the existing protections. ABC also analyzes and documents the design and operation of the existing suite of policies, procedures and internal controls designed to secure and/or limit access to that trade secret. Through this process, ABC's management becomes aware of potential gaps—vulnerabilities—in its existing compliance/security architecture that may require new investment to strengthen and/or enhance efforts to mitigate the risks associated with the combined threat and vulnerabilities. They also identified processes within their trade secret protection management system that were weak and would require improvement. ABC leverages a traditional risk and control matrix to document its analysis, thereby facilitating a discussion with management; an abbreviated example is included as Figure 6

Figure 6: Threat and Vulnerability Matrix

Trade Secret	Threat Actors	Probability of Trade Secret Theft Event (high, medium, low)	Severity of Trade Secret Theft Event (high, medium, low)	Existing Policies, Procedures, Controls, and Mitigating Actions	Severity of Trade Secret Theft Event (high, medium, low)
Source Code	• Nation state X • Competitor Y • Competitor Z	High	High	• Information Security policy • Limited access to local development group, November 2013 • Source code located on a secure server • Access control list to source code • Document handling standard	Medium • We lack a consistent training program • We have found instances of source code being circulated • We have not conducted attack and penetration testing against our servers in the past year.

Protecting Trade Secrets: At What Cost to Collaboration?

Companies often raise concerns that taking steps to limit access to trade secrets by implementing stringent security measures has the inadvertent effect of creating "work arounds" in which employees create unofficial processes and means to access trade secrets so as to avoid encountering the security measures—for example, mandating a highly complicated password to access sensitive documents leads to employees writing the password on a note and keeping it in their desks where other staff may find it. While this would be a violation of company policy, employees may be doing so in order to "get the job done", collaborate, and operate efficiently.

Companies must select the appropriate level of security controls for their unique corporate culture, the amount of time and resources to be invested in training and awareness campaigns. Once these issues are addressed, create clear policies and processes articulating the responsibilities of individual employees. Compliance monitoring and periodic analysis should also be implemented.

For example, since many of ABC's trade secrets relate to its source code, its vulnerability analysis targets the security of its information technology systems and the access controls surrounding the systems. ABC engages in discussions with its CISO, who identifies the security controls that are currently in place for the identified systems. They debate whether these controls are well understood by company employees, and review policies and training programs that support them. The team discusses the potential vulnerabilities of each level of protection given the known and suspected threat actors who may be targeting the company.

The cross-functional team responsible for the overall trade secret protection management system begins to realize the difference between IT security and trade secret protection. This major realization impacts how they proceed to develop a plan that integrates both. At this stage, ABC acknowledges these vulnerabilities and develops recommendations for enhanced mitigation.

Level 3: Trade Secret Portfolio Relative Value Ranking

With only limited resources to implement new safeguards around its most critical assets, how should management decide which trade secrets deserve greater protections? How should management rank its trade secrets based on the insights garnered from the initial analyses performed in Levels 1 and 2?

A Relative Value Ranking analysis provides the company with the means to conduct a qualitative assessment using value-based judgments on the relative importance of a trade secret so that it can perform an initial selection of trade secrets that have the most significant impact on the operations and performance of the business.

Following completion of Level 1 and Level 2, management has new and critical insights into the scope and extent of their trade secret portfolio, including potential areas of vulnerability and threat actors who may seek to inflict economic harm on the company. Depending on the company, these analyses may have provided insights into dozens of trade secrets that the company maintains; some of which are clearly more valuable or create more exposure than others. This value ranking is a critical in developing a return on investment (ROI) proposition that management can use to justify investing more resources in trade secret protection and IT security.

Figure 7 provides an illustrative series of questions to aid management's ability to prioritize those assets among its trade secret portfolio based on the insights from Levels 1 and 2. A related scoring methodology then yields a ranked version of the portfolio based on management's risk assessment of the assets. In order to safeguard the ranked list, companies may consider putting the process and ranked results under attorney client privilege to prevent a defense team from later claiming in court that lower value trade secrets should translate into lower value damages awards.

Following completion of its Level 1 and Level 2 analysis, ABC's Compliance Counsel gathers ABC's executives to evaluate the questions in Figure 7 and rank each asset. For each trade secret, ABC uses these questions to assess the dimensions of the asset's value to the business. In this instance, the relative weights of "Low",

Figure 7: Establishing the Relative Value Ranking for Company Assets

	High	Medium	Low
How significantly would the company's reputation be impacted if this trade secret were compromised?	We would have devastating reputational impacts	We would likely have some reputational damage that we would have to respond to and manage	Not very, may have some residual effects but we could recover from them
How critical is this trade secret to the fundamental operation of the business?	It is absolutely critical and there are no viable alternatives	It is critical but we could find an alternative if absolutely necessary	It is not critical to our business operations
How core is this trade secret to our corporate culture that its loss or theft would have a strong emotional impact on the corporate culture?	This is at the core of our culture and would have a devastating impact on morale and our identity	This is core to our business and its loss would be felt by our employees but we would recover fairly well	It is not a core component of our corporate culture
Is this trade secret especially unique to the industry or is a similar product being used/sold?	We are the only company in the industry that makes/sells/uses this	Other companies make/sell/use it but our version has an exceptional characteristic that makes it unique	No, many other companies make/sell/use something similar
Could competitors place a higher value on this trade secret than we do?	Yes, this can be used for many more purposes that we use it for and therefor	Maybe, but we are unaware of how it may be valued differently	No, its value is consistent across the market
How important is this trade secret to current or projected revenue?	It is critical to current and/or future revenue and would be nearly impossible to replace	It is important but we are sufficiently diverse that we could make up the difference if pressed to do so	Not very important or we haven't determined its importance

"Medium" and "High" were calibrated for each category (assessing, for example, the relative reputation cost of a "High" impact in the first column vs. a "Medium" impact) and then the overall asset scores combined. This exercise results in a ranked analysis of ABC's trade secrets by relative value, wherein higher scores are associated with trade secrets that are deemed more important or valuable than other trade secrets in ABC's portfolio. Deciding how appropriately to allocate resources to protect assets is not only dependent upon the relative score, but also an assessment of the economic impact should that trade secret be stolen. Accordingly, ABC's Compliance Counsel decides to proceed to the next level of the framework to assess the economic impact of a trade secret theft event for the ten trade secrets that ranked highest in this exercise.

Level 4: Economic Impact Attributable to Trade Secret Theft

In this Level, management will seek to assess the economic impact of a trade secret theft event for the company's most valuable trade secrets identified in Level 3. Applying both quantitative and qualitative analyses, management will calculate the potential economic losses attributable to theft and, leveraging results from previous Levels, adjust the economic loss analysis based on the perceived threat.

4.1: Impact Assessment

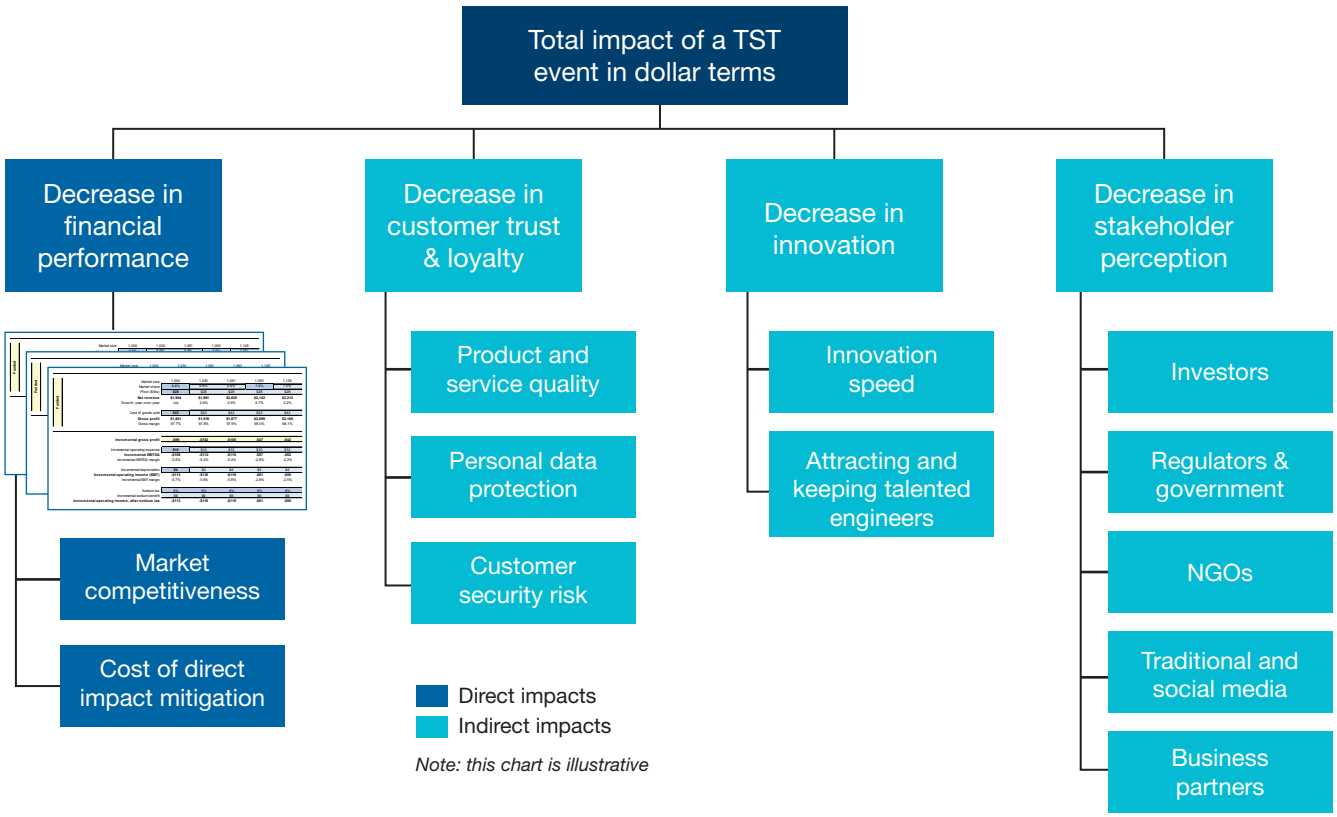
In this step, the company determines the adverse economic impact to the company if an individual trade secret asset is misappropriated. This process enables management to segment the total impact into manageable building blocks and understanding of both direct and indirect impacts helps to establish a complete picture of the economic losses attributable to a trade secret theft event.

- ***Direct Impact:*** A measure of the direct financial and economic losses attributable to a trade secret theft event—i.e., lost sales/revenues, lost market share, lost profits, and/or lost economic opportunity; and
- ***Indirect Impact:*** An assessment of the indirect factors impacting a company's short/long-term ability to compete in the marketplace due to the theft of the output of its investment—e.g., reduction in customer trust due to concerns about ongoing relationships or adverse press impacting the company's reputation in the marketplace.

In this context, it is important to consider both the direct and indirect aspects of a trade secret theft event to help companies capture the full range of economic exposure that threat actors' actions may impose on the organization. The results of the impact assessment provide the basis for establishing a ROI proposition for improving trade secret protection. In most companies, compliance is seen as a cost, not an investment. The valuation is critical to helping companies understand that improving trade secret protection is an investment that has a quantifiable ROI.

In this phase of the framework, ABC's Compliance Counsel may begin by conducting workshops with executives overseeing major subsidiaries or key business units and leaders of core corporate functions (e.g., finance, technology, sales/marketing, human resources) to map areas in which a trade secret theft event could adversely impact the value of the company's operations and business/market environment. A model for these discussions is reflected in Figure 8.

Figure 8: Economic Impact of a Trade Secret Theft (TST) Event



4.1.1: Direct Impact

Estimation of the direct financial impact from the theft of trade secrets is grounded in traditional discounted cash flow analysis that many companies use every day to make business and investment decisions. This estimate typically focuses on various factors including revenues, costs, and profit analysis. It may assess trade secret theft's impact on a company's market competitiveness, or the costs of impact mitigation actions:

- ***Adverse Impact on Market Competitiveness:*** Applying traditional discounted cash flow analysis to estimate the reduction in market share, revenue and profitability due to factors such as business interruption and/or dislocation after a trade secret is stolen, loss of potential licensing revenue, or loss of competitive differentiation; and
- ***Cost of Direct Impact Mitigation Actions:*** After an event, companies may take action to mitigate negative consequences and restore their competitive position or reputation in the marketplace (e.g., litigation against the responsible party). The costs associated with these actions should be included in this element of the estimate.

ABC's management identifies a range of threats related to potential exposure of particular trade secrets. Examples include, but are not limited to, the following:

- *A competitor could steal ABC's source code to re-engineer a product, discount its prices and still generate a profit because it would not have to cover the return on R&D efforts. Based on a market analysis, management can estimate what level of market share, revenues and profit would be lost.*
- *If threat actors compromise the production server for a key service that generates business through continuous micro transactions, the server can go down. Until the company restores operations it would lose revenues. The customer service department would likely work overtime to manage client complaints, and the company might need to prepare and deliver messaging related to the disruption. Management could estimate these lost revenues and additional expenses.*
- *If threat actors hack ABC's servers and gain access to "sensitive business information" related to ABC's supply chain that compromises the supply chain's ability to compete in the marketplace, suppliers could decide to take legal action against ABC if it appears ABC acted negligently in handling suppliers' trade secrets. Such legal action could contribute to increased legal fees and associated costs for ABC. ABC's legal department could make a reasonable estimate of the nature and amount of these costs.*

Applying these concepts, ABC management estimates the direct financial impacts for the top ten trade secrets in its portfolio identified in the Level 1 exercise.

4.1.2: Indirect Impact

Companies must also consider longer-term, indirect adverse changes to their business environment resulting from trade secret theft. As noted above, these issues typically involve qualitative but nonetheless critical impacts to the organization (e.g., customer relationships, reputational matters) that can be thought of as key drivers of company value. The common element of these indirect impacts is that they are strategically important for the company, but the extent to which they drive financial performance is typically difficult to quantify.

In this context, ABC identified several areas in which a trade secret theft event will adversely impact their business.

- ***Customer Trust and Loyalty:*** *ABC believes a trade secret theft event would negatively impact the trust and loyalty the company experiences with certain customers who value the company for product quality and safety. If ABC cannot protect its own assets, customers may doubt that their own confidential information (e.g., design specs) is adequately protected. Customers may express further concerns about a threat actors' ability to access their own systems through the compromised source code. Such factors may decrease customer's willingness to engage with ABC, thereby reducing long-term revenues and profitability.*

- ***Innovation and Talent:*** *ABC's key competitive advantage lies in its innovative approaches and its ability to develop new alternative energy solutions that provide value to customers. If source code is stolen, the company's pace of innovation may stall as enhanced security measures are adopted, requiring engineers to adapt to new policies and procedures. Key engineers may leave the company, or it could become more difficult to recruit new talent. Further innovation processes may be cut back. Collectively, these factors could lead to decreased innovation and subsequent reductions in long term performance.*
- ***Stakeholder Perception:*** *ABC works with multiple stakeholders who influence markets and customers, so maintaining the trust of the company's stakeholders in ABC's security protocols is essential. For example, investors may assert that the company lacks appropriate controls and protection processes to support sustainable growth, deciding to sell shares despite the absence of direct financial consequences of the theft. Also, if discussion of the theft trends on social media blogs or is covered by traditional media, it can influence long-term customers' buying decisions. Similarly, the theft may erode the trust of the company's key business partners.*

Such indirect impact areas all bear upon areas of strategic importance for the long-term performance of companies. To facilitate assessment, companies can consider Key Performance Indicators ("KPI") for each identified indirect impact area and convert them into dollar terms using Multi-Attribute Utility Analysis ("MUA") to measure the economic impact on the business. Specialists familiar with the identified indirect impact areas can inventory existing KPIs and/or create new KPIs to measure performance. While the values generated do not represent accountancy measures, indirect impacts can be converted to economic costs, allowing comparisons of prioritized trade secrets' direct and indirect impacts. This will also help measure the benefits of potential actions companies could take to protect their trade secrets further, as discussed later in the paper.

For example, ABC may convene discussions to identify KPIs across all the identified indirect elements. The company's customer surveys and market surveys targeting future customers include questions that focus on customer trust and loyalty. Management estimates how these survey results would change in case of a trade secret theft event for each of the prioritized trade secrets. With these measures available, MUA techniques enable ABC management to construct a model expressing the economic costs of each KPI, making it comparable to the direct financial impact estimate.

4.2: Threat Adjusted Economic Impact

The Impact Assessment (Level 4.1), Threat Actor Analysis (Level 2.1), and Vulnerability Analysis (Level 2.2) are aligned to form a total "Threat Adjusted Economic Impact" value for each trade secret and across the portfolio. Collectively, these considerations inform management of the potential threats facing individual trade secrets with a clear view of where the impacts would be, how likely a threat is, and how protected the company is against them. This information enables management to allocate resources across the portfolio to adequately safeguard these important assets – the next level in the framework

For example, an important trade secret in ABC's portfolio is inherently valuable to the company, but the threat actor analysis indicated that marketplace demand among threat actors for this trade secret was low and the company's existing procedures and internal control were adequate to mitigate potential exposure. Conversely, ABC's management determines its source code is equally valuable, yet its exposure to threat actors would inflict significant economic harm to the company. ABC's analysis further indicates that new working practices and internal controls would enhance ABC's ability to mitigate potential threats in this area.

Level 5: Protective Action Portfolio Management and Allocation of Resources

Analysis of the Threat Adjusted Economic Impact for those trade secrets deemed most important to a company enables management to make informed decisions about how appropriately to use its existing resources to strengthen its ability to mitigate potential threats through advanced protective measures. With insights into the economic costs of a potential trade secret theft event in hand, management can effectively assess the incremental costs of developing and implementing a trade secret protection management system. This can include including new policies,

procedures and/or internal controls against the perceived threat, and the appropriate allocation of resources. For example, the benefit of new protective actions (e.g., impact mitigation, reduced exposure to threat actors, strengthened access controls) can be measured through the reduction in the Threat Adjusted Economic Impact for a single trade secret or across the portfolio, if the benefit extends to multiple trade secrets. Collectively, this approach enables management to effectively analyze its existing resources and efficiently reallocate those resources to safeguard the company's most important assets; in turn, aligning resources with the company's broader strategic priorities and objectives. The cost of developing and implementing a trade secret protection management system can also be established, thus allowing the company to assess the ROI.

ABC, after completing the previous levels of the framework, has a clearer understanding of which trade secrets are at highest risk of exposure, and how exposure would impact its operations. Now, through a series of workshops with subject matter experts, management lists a series of action items that various parts of the organization planned to protect the selected trade secrets. Some of the identified actions focus on the following areas:

- *IT would raise the company's protection level by establishing new servers and firewalls and ensuring all software is routinely updated;*
- *The product development teams would develop multiple plans to segregate and limit access to source code in order to mitigate the adverse economic impact if one piece of source code were stolen;*
- *The public relations and customer service teams would design "emergency" protocols with which the company can quickly react and communicate to the market and key stakeholders in case of a trade secret theft event. Such a response would help mitigate adverse changes to customer trust and perception of key stakeholders.*

In this process, ABC's management team evaluated the recommendations for advanced protective measures around each of the trade secrets and, within its pool of available resources (e.g., budget, talent/personnel, and capabilities of existing information technology systems), targeted mitigation strategies where the enhanced protective measures would lead to the highest reduction to an individual trade secret's Threat Adjusted Economic Impact. This enabled the company to measure the ROI on each action and select the appropriate portfolio of actions to increase the ROI given the company's available budget.

On this basis, management constructed a briefing to senior executives and ABC's Board of Directors to convey their observations of ABC's trade secret portfolio, potential threat actors targeting the company and exposures identified in the vulnerability analysis. The briefing included recommendations to mitigate these emerging threats, including an improved trade secret protection management system, consisting of new policies, more effective procedures and infrastructure-hardening controls. The recommendations were grounded in an economic assessment that balances incremental costs against expected returns. ABC's management plans to perform this analysis annually to help to establish that the company's compliance and security efforts align with the changing market environment and evolving strategic priorities of the company.

This framework addresses the key components of a company's strategy to protect its trade secrets—identification of the secrets, clarification of where and how they are stored or protected, and informing management's ability to make effective and efficient decisions on how to adequately deploy protection measures based on meaningful economic analyses. Applying this framework is a significant undertaking for any company, particularly those approaching these processes for the first time. Stratifying the framework into discrete levels allows companies to take an iterative approach to safeguarding their trade secrets, in order to marshal the necessary resources, obtain buy-in from key stakeholders, evaluate progress, and gain consensus at each level before continuing. Completing each level should be considered significant progress for any company that undertakes this effort.

How do Expectations of Future Trade Secret Loss Impact Private Sector Decision-Making Today?

Corporate executives around the world regularly make decisions based on expectations about the future. Choices related to new product launches, expanding strategic business relationships, investment in capital projects, and research and development expenditures are each grounded, in part, on companies' expectations about the future. Effective management of a company's trade secret portfolio requires a similar perspective.

- Will the identified trade secret provide the company with a competitive advantage in the marketplace? For how long? What level of economic returns will these trade secrets provide? Over what period of time? How will the company capitalize on this investment in the marketplace?
- How will the company protect these trade secrets from internal and external threat actors to promote the anticipated competitive advantages and returns in the marketplace are achieved? Are new compliance and security protocols required to safeguard the investment during this phase? What is the plan to improve the maturity of the trade secret protection management system and the information security program? How are those costs factored into the expected economic returns?
- How will expectations involving external factors—regulation, openness of the Internet, cybersecurity threats, emerging threat actors in the marketplace, the pace of innovation—drive the company to evaluate the diversity of threats and incremental costs associated with protecting its trade secrets? How can improved trade secret and IP protection be used as a competitive advantage in the global marketplace in attracting customers, partners and investors?

For years, executives have asked questions like these as part of their internal analysis and due diligence around new investments in R&D projects where the investment's expected time horizon for a return extends for several years. In today's marketplace, however, these questions are increasingly important given the emerging threat of trade secret theft and the prevalence of other forms of economic crime that can adversely impact the economic analyses upon which these investments are based. Accordingly, corporate executives are increasingly focused on analyzing potential future scenarios and the consequences of acting (or choosing not to act) to further protect the development of their trade secrets; especially for significant capital investments with extended periods before economic returns are generated.

In 2013, the U.S. Intellectual Property Enforcement Coordinator wrote in its strategic plan on IP enforcement that, "As we move forward, we are aware that new technologies, evolving social norms, new business models, and novel global distribution mechanisms will present new challenges and opportunities to combat infringement of American intellectual property rights."[39]

New challenges and opportunities form the basis of the following section of the report. We modeled three scenarios focused on trade secret protection-related issues over the next 10-15 years. The scenario models are not predictions; but rather projections of possible outcomes based on a narrow combination of drivers. They are intended to challenge assumptions and provoke new thinking about this issue and where it might go in the future.

As part of this scenario modeling effort, we convened panels of subject matter experts from leading companies, law firms that focus on patents and trade secret protection, and personnel from think thanks and academic institutions that focus on trade secret theft and global change. These subject matter experts provided insights on the challenges and opportunities for companies to consider in each of the three scenarios. They also offered mileposts and indicators that would be observable in the real world that might indicate one scenario or aspects of one scenario could become more likely than others.

Key takeaways from our modeling sessions include:

1. ***Trade secret protection must increasingly focus on external threat actors who may have designs on stealing critical trade secrets and IP.*** However, in the present world and going forward, the insider threat will continue to be a dangerously rich source of trade secret loss.
2. ***Changing social norms, especially a country's cultural expectations of the degree to which companies must disclose confidential and commercially sensitive information, will significantly impact trade secret protection in the years ahead.*** When considering countries for expansion or new market entry, companies may factor how the government and the culture generally treat secrets, as well as the extent and nature of protections the company can expect to receive if its trade secrets are misappropriated.
3. ***The openness of the Internet will have a significant impact on how companies develop and protect trade secrets.*** If separating or walling off from the Internet becomes politically and socially accepted, we may see some trade secrets—built on an assumption of an open and thoroughly interconnected world—decrease in value.
   - In the latter half of 2013 some multinational corporations and national governments publicly raised the issue of segmenting or walling off parts of their Internet traffic.
4. ***Sectors that are able to band together and share threat information concerning trade secret protection will likely fare better than sectors in which participants remain combative and distrustful of peer organizations.***
   - Intra-sector intelligence sharing already pays dividends in some sectors of the economy; more sectors may pursue this collaborative approach in order to better enable trade secret protection in the coming 10-15 years.

Drivers and Scenarios

Numerous drivers and forces will have an impact on trade secret protection in the coming 10-15 years. For our futures section we selected four drivers that will likely impact these futures and that, in different combinations, offer compelling lessons and different visions for us to consider from our current vantage point.

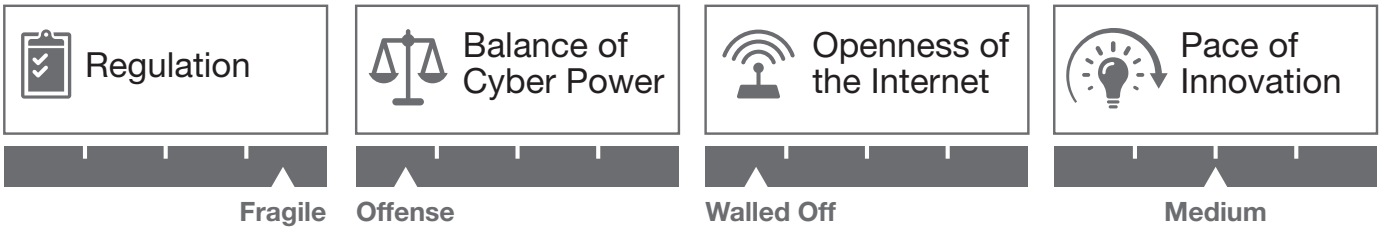
Driver 1: Regulation for the protection of trade secrets: Enhanced global regulation could take hold to increase protection of trade secrets. Alternatively, a future in which no such regulation emerges could be one of increasing collective and individual vulnerability for companies, individuals, countries and other global players.

Driver 2: Balance between cyber offense and defense: A defense-intensive environment would be characterized by its clear, unambiguous ability for attribution of cyber activities and dramatically improved cyber defense systems. A tilt towards the cyber offense would not only mean that threat actors would have the upper hand technologically, but that individuals and companies may be more willing and able to launch cyber attacks on their own.

Driver 3: Openness of cyber commons vs. "walled gardens": The openness of the Internet could remain the status quo for the next 10-15 years. An alternative would be the emergence of walled gardens or the creation of IT networks that are separated from the wider Internet. Walled gardens could be used and created by cities, sectors or countries.

Driver 4: Pace of innovation: The final driver considers the rate at which new ideas are developed and spread across the global economy. Innovation is a key foundation of much of what drives the creation of trade secrets. In futures with a faster pace of innovation, there could more trade secrets.

Scenario 1: "Shelter in the Storm"



In this future, the absence of a robust regulatory framework and international consensus on means for trade secret protection—including but not limited to cybersecurity—combines with offensive cyber capabilities having the upper hand.

Fears of intelligence-gathering by governments, dramatically increased data-theft by criminals, and a series of devastating global cyber attacks creates pressure for individuals and corporations to wall their information off from a dangerous world. In addition to this fear there is a definitive tilt in the balance of cyber power towards those who are on the offense, leading to periodic spikes in cybercrime and cyber-enabled economic espionage. This tilt to the offense is a dual-edged sword, as social norms and the lack of regulation make it easier for some companies, individuals and groups to periodically go on the offensive themselves, launching carefully honed cyber attacks at assessed threat actors.

The perceived dangers to trade secrets and intellectual property on the Internet and connectivity in general lead to new coalitions seeking to increase their security through collective measures. By the end of this 10-15 year period, some companies and sectors have begun to combine forces—sometimes by sector, nation, state or country—behind separate Internet systems that become known as walled gardens.

Information blocs of countries and industries become prevalent. Data centers—formerly globalized—now are owned by groups of countries and hosted in shared locations under the terms of multilateral agreements that exclude non-members.

Eventually, there is some expanded exchange and trade among members of these cyber-blocs. Global commerce decelerates though, and firms with extensive cross-border operations suffer as their ability to conduct data transfers is restricted. Customers prefer to "buy local," reducing firms' need for competition-driven innovation and reducing the value of many trade secrets. Some companies decide to stay outside the walls for a variety of factors.

The observations of many subject matter experts (SMEs) related to this scenario focused on the unique challenge of the walled garden as an active element of this future possibility. SMEs agreed that this world is one of significant adjustment for governments, companies, individuals and even threat actors.

Challenges

- Organizations will face higher costs if they choose to wall off and separate from the open Internet; smaller entities may not be able to survive.
- Global regulations and standards would suffer and be replaced by limited agreements within walled gardens or between walled gardens.
- This world will feature high transaction costs and slower advances in technology.
- Inside the wall, companies will be less agile and will realize fewer gains.
- The high barrier to investment and cooperation outside the walls may lead to lower levels of investment and loss of trade opportunities.
- Being in the walled garden would limit companies' choices of suppliers, employees, service providers and customers.

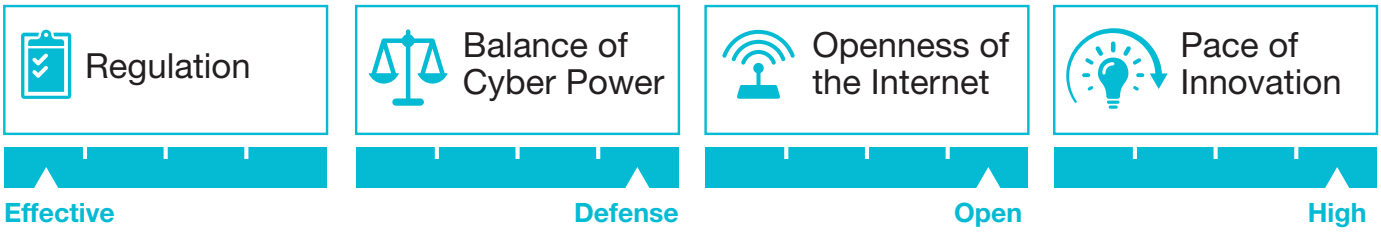
Opportunities:

- Within the gardens, there will be greater security, but at the cost of agility. Those outside the walled gardens will face higher risks, but will also have chances to reap higher rewards.
- Within the walled gardens, especially larger more diverse gardens, there would be numerous opportunities for some sectors to flourish given the high degree of protection from cyber-enabled economic espionage.
- The need to abandon the current model of leveraging overseas talent and distributed supply chains can provide new opportunities for companies to do work that is perceived as more secure though perhaps more costly.
- Companies with a rapid R&D and product development cycle might choose not to wall off, instead remaining in between the walled gardens even if this meant operating at a higher state of risk in order to provide the greatest freedom of movement despite potential increased threats.

Mileposts:

- Quantum computing capabilities to advance the shift of cyber power towards the offense.
- A key member of the G8 or G20 walling off parts of its Internet.
- A series of devastating cyber attacks on trade secrets and IP.
- Governments and companies are unable to gain the advantage on cyber attackers and are constantly behind the curve.

Scenario 2: "The Roaring 20(20s)"



Open cyber commons, combined with a tilt towards stronger cyber defenses, produces a scenario in which companies are increasingly able to protect trade secrets and consequently undertake collaboration, joint ventures, and investment with greater confidence.

Because of the balance of cyber power towards the defense, the private sector at times becomes complacent about security, discounting emerging threats and short-changing security measures. This results in occasional intense bursts of cyber attacks against entire sectors when threat actors find chinks in the technological armor. Public-private partnerships—partly the result of more effective and far-thinking regulation on trade secrets and cyber security—and strong intelligence cooperation within sectors limit such outbreaks to manageable proportions. Companies cooperate to drive a culture of compliance into the global supply chain—upstream and downstream. Trade secret protection management systems are implemented and become as common as quality management systems.

Effective regulation in a defense-intensive environment pushes malicious activity to the fringe and reduces the incentive for criminal efforts to steal trade secrets, while not entirely stopping sophisticated efforts by intelligence services and mature organized criminal networks.

The moderate pace of innovation fosters the creation of new trade secrets and intellectual property. Global trade and commerce steadily progress.

Many SMEs were cautious about the Roaring 20(20s) and were careful to point out that even such a seemingly safe place as this world would come with a cost for many companies.

Challenges:

- Organizations will seek to abuse a stronger regulatory environment by mounting frivolous lawsuits.
- Smaller companies without the resources to deal with new regulation or a harsher litigation environment might be challenged to stay in business.
- The decrease in cyber attacks and a tilt in the balance of cyber power towards the defense may make some companies complacent about security and more vulnerable to attacks from cyber actors and insiders.

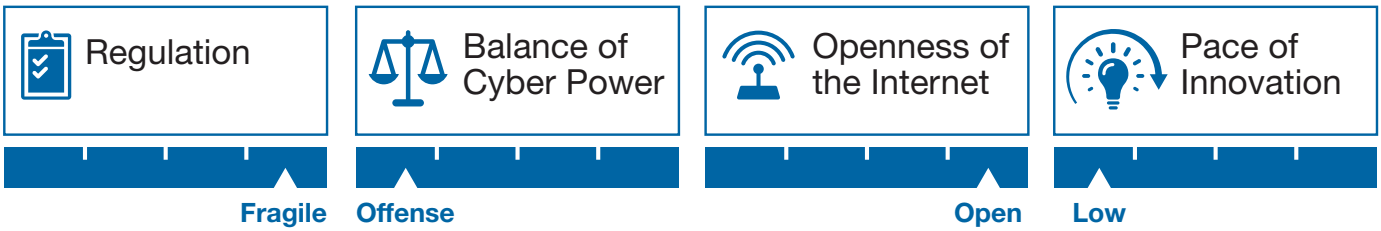
Opportunities:

- If the regulatory regime were truly effective in protecting trade secrets, then the Roaring 20(20s) might witness a golden age of trade secret protection.
- If cyber systems are more secure, companies can focus on policing negative employee behavior, such as the rise of the insider threat. They can continuously improve their trade secret protection management systems.
- Smaller companies may increase their flow of new ideas and trade secrets into larger companies to take advantage of larger companies' regulatory processes and protections.
- Large companies could cooperate to improve respect for trade secrets in their end-to-end supply chains.

Mileposts:

- Significantly increased public outcries about trade secret theft leads to the emergence of a regulatory framework—particularly national-level statutes—that would clearly demonstrate an ability to help companies protect trade secrets.
- Actions by the U.S. Government or other governments to share more clearly defined cyber information and intelligence with the private sector or change laws to enable national-level cyber systems to act as both cyber shield and sword for the private sector, thereby gaining the cyber offensive against threat actors.
- A consistent string of defensive victories against threat actors known to target trade secrets that would be devastating enough to keep them on their heels for extended periods of time.
- Signing and enforcement of global agreements curtailing economic espionage.

Scenario 3: "Radical Transparency"



In this world, regulation and norms on trade secret protection break down, leaving it to individuals and companies to decide when to put up fences, when to steal trade secrets, and when to retaliate for cyber intrusions. The balance tilts in favor of cyber offense, resulting in rapidly emerging threats to trade secrets from individuals and small networks.

Governments can offer little protection other than lip service to the mounting losses. Regulations and customer expectations work to keep corporations or countries from creating walled gardens as an option to protect trade secrets and other IP.

The private sector has little choice other than to adopt an open and transparent collaboration model because widely shared innovation-to-market practices are the norm as the only way to meet customers growing expectation of rapid delivery.

Those launching cyber attacks have the consistent edge in the Radical Transparency world and the high cost of protecting trade secrets disincentives private-sector R&D in some sectors. Some governments try to pick up the slack in R&D in goods and services related to defense, pharmaceuticals, and public health. The effects of slackening R&D are evident only towards the end of the period as the flow of new technologies becomes dramatically slower.

Governments and multinationals exert decreasing influence as "radical transparency" accelerates the power of existing societal forces such as WikiLeaks, grass-roots anti-corruption movements, and new "third forces" gain traction. Transparency advocacy groups' cyber and political power grows and provides them with a platform to pressure companies and governments for transparency above protections for trade secrets.

Many subject matter experts felt that the balance of drivers laid out in this scenario would be the "storm" that might predate the future described in our first scenario, "Shelter in the Storm." Other SMEs opined that this future is, in some ways, not far off from the status quo. Lastly, some SMEs independently concluded that this world would be welcomed by some of the largest Internet-related products and services companies given their interest in openness and transparency.

Challenges:

- For businesses this is a hypercompetitive environment for resources, talent and opportunities.
- Given the hypercompetitive environment smaller firms may not do well in this future.
- Some organizations may seek to act preemptively against perceived threats, and might feel freer to use cyber weapons against known or suspected threat actors.

Opportunities:

- Academic institutions and non-profits, which have long emphasized transparency, would become more influential compared to the present day.
- Given the balance of cyber power and the increasing acceptance of transparency, non-electronic document delivery systems, such as couriers and package delivery companies, might see their services expand for businesses that will not risk electronic networks lest their information might be divulged by those seeking transparency or to steal the information.
- Some companies can band together to share information face-to-face as some sectors have done. The financial sector's creation of the Financial Services Information Sharing and Analysis Center ("FS-ISAC") is a good example of what we might see more of in this future.

Mileposts:

- Organizations that champion transparency gain sponsorship from global leaders or G20 countries, or find champions from leaders of similar stature.
- Use of stolen data becomes more accepted, driven by changes in social norms.
- National and international regulations and treaties on trade secret protection flounder and fail.
- A sustained mass movement against trade secrets or corporate secrecy that gains traction beyond the fringes of political circles.

Key observations from scenario modeling exercise:

Companies and industry associations should consider new and innovative ways to come together to think about the road ahead for trade secret theft, and to identify the drivers that will impact trade secret protection in their areas of concern. The drivers used to construct these three scenarios represent only a fraction of the many influences that will shape how trade secrets are protected and misappropriated in the next 10-15 years. Additional forward-looking analyses that consider how threats to trade secrets may evolve may illuminate other critical drivers. Such efforts will spark debate and discussion about which drivers companies, governments and individuals can influence most effectively in order to create more security and stability for their interests and assets.

Please note that the possible opportunities and challenges summarized in our scenario modeling exercise can be replicated or supplemented by individual companies to help them prepare for a variety of future outcomes and to be ready to act decisively to make the appropriate and most secure use of their intellectual property and trade secrets, regardless of what future emerges. By understanding how trade secret misappropriation and other aspects of trade secret protection, including trade secret protection management systems, may develop in the next decade, companies can incorporate these trends into the framework analysis documented earlier in this study.

Conclusion

The trade secret evaluation methodology provided in this report can provide a first step in a larger collective effort to improve trade secret protection, and help companies to better appreciate the importance of proactive protection as an up-front investment. At the company level, firms would benefit from a better understanding the relative value of their trades secrets and the harm that any loss or theft would inflict on them. Understanding the probability and severity of a potential breach can better inform decisions on investments and other critical activities. We hope this also encourages and inspires companies to be more forthcoming in discussing the challenges associated with trade secret protection, thus advancing a broader dialogue on this issue.

This report also provides a glimpse into three possible futures concerning trade secret theft. In addition to demonstrating the breadth of situations that companies must consider and plan for, such a modeling exercise is particularly critical in an era where technology, policy, customer demand and innovation are making trade secrets ever more valuable to those who create them as well as those who wish to steal them. Companies that fail to anticipate the evolution of threats, regulation and other key drivers risk falling behind their competitors and losing market share.

There is increasing convergence between concepts of privacy and data security generally and trade secret protection. The measures that consumers use to protect their personal information overlap significantly with measures that companies take to protect their trade secrets (e.g., consumers and employees not falling victim to spear-phishing scams; not storing sensitive information in the "cloud"). The more that companies can emphasize that their trade secret protection measures can be used to protect personal privacy, the more acceptances may be gained in employee populations. This may occur on a national level as well as a company level.

The challenge of trade secret theft is too large for any one government, company or organization to deal with alone—only a collective focus on this issue will help improve innovators' ability to secure their most critical information and intellectual property. This cooperative effort will be strongly aided by the investment of individual companies' time and resources to help to establish they know who threatens their own interests and how to measure the value of their own trade secrets. Replication of this sort of increased self-awareness across entire sectors would produce a detailed understanding of the collective threats and challenges, and the thorough extent of the value of trade secrets. Private sector companies—and other targets of trade secret theft—should approach this issue with a sense of urgency. Threat actors show no signs of slowing their attacks on trade secrets, and each new advance in technology brings new potential vulnerabilities with it.

"An environment where it may be easier to steal a vital intangible asset than it is to value, disclose, or even realize its loss is an inherently risky one."

– PwC Global Economic Crime Survey, 2014

Acknowledgements

This report represents the analysis and efforts of many individuals within CREATe.org and PwC. This publication was produced under the direction of Pamela Passman and Leslie Benton from CREATe.org and Sanjay Subramanian and George Prokop from PwC. Our report was created and coordinated by Marissa Michel, Craig Stronberg and Peter Geday.

During the drafting of this report, we consulted with numerous subject matter experts in the private and public sectors who participated in our threat modeling workshops and reviewed our final draft. We also would like to thank Roberto Rojas for his assistance.

Endnotes

1 "Economic Espionage Act of 1996" Published by the U.S. Government

2 Article 39 of the World Trade Organization's Agreement on Trade Related Aspects of Intellectual Property Rights ("TRIPS") states: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or Used by others without their consent in a manner contrary to honest commercial practices so long as such information: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

3 The Center for Responsible Ethics And Trade ("CREATe.org"), Trade Secret Theft: Managing the Growing Threat in Supply Chains (May 2012)[please add link]

4 "The 2012 Statistical Abstract/National Data Book. Patents and Trademarks: 1990 to 2010," Census. Bureau, U.S. Department of Commerce, 2013

5 "The Report of the Commission on the Theft of American Intellectual Property", 2013

6 "Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods", General Accountability Office, April 2010

7 Ibid

8 National Science Foundation, National Center for Science and Engineering Statistics. 2013. National Patterns of R&D Resources: 2010–11 Data Update.

9 2013 and 2013 Global R&D Funding Forecasts, *Battelle.org* and *R&D Magazine*—December 2012 and December 2013

10 The Battelle Foundation, "2013 Global R&D Funding Forecast," December 2012

11 Justin Hicks and Robert D. Atkinson, "Eroding Our Foundation: Sequestration, R&D, Innovation and U.S. Economic Growth," The Information Technology & Innovation Foundation, September 2012

12 Association of Certified Fraud Examiners ("ACFE"); "Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study"

13 Treasury Inspector General For Tax Administration: Office of Inspections and Evaluations, "The Internal Revenue Service Needs to Improve the Comprehensiveness, Accuracy, Reliability and Timeliness of the Tax Gap Estimate," August 21, 2013

14 Myths and Realities of Governance and Corruption, Daniel Kaufmann, World Bank, October 2005

15 Business Software Alliance, 2012, "The Shadow Market: 2011 BSA Global Software Piracy Study: Ninth Edition"

16 U.S. Department of Justice: The Economic Impact of Illicit Drug Use on American Society, 2011

17 Havocscope: Global Black Market Information; "World Black Market Value", December 2013.

18 Illicit Financial Flows from Developing Countries: 2002-2011. Dev Kar and Brian LeBlanc. Ford Foundation, December 2013

19 Office of the National Counterintelligence Executive ("ONCIX"), "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011", October 2011, published by the Office of the Director of National Intelligence

20 Office of the National Counterintelligence Executive ("ONCIX"), "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011", October 2011, published by the Office of the Director of National Intelligence

21 Ibid

22 Ibid

23 "Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets," U.S. Department of Justice, December 21, 2011.

24 RJGG v Director General of Security [2013] FCA 269 (Federal Court of Australia, Foster J, 27 Marcy 2013)

25 PwC, State of Cybercrime Survey 2013; State of Cybercrime Survey 2012

26 Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." February 2013

27 Office of the President of the United States, "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets." February 2013

28 Ibid

29 Katherine Herbig, "Allegiance in a Time of Globalization," Defense Personnel Security Research Center, December 2008.

30 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013

31 Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, February 2013

32 "White House Strategy to Combat Transnational Organized Crime", The White House, July 19, 2011

33 Organized Crime and Cyber-Crime: Implications for Business, Phil Williams, CERT® Coordination Center

34 Office of the Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," March 12, 2013

35 Raj Samani and Francois Paget, "Cybercrime Exposed: Cybercrime-as-a-service," McAfee.

36 Dr. Mike McGuire and Samantha Dowling, "Cyber crime: A review of the evidence. Research Report 75. Chapter 1: Cyber-dependent crimes," Published by the United Kingdom Home Office, October 2013

37 Office of the Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," March 12, 2013

38 Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases, U.S. Attorneys' Bulletin, November 2009

39 U.S. Intellectual Property Enforcement Coordinator, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT, June 2013. Published by the U.S. Government

www.create.org

www.pwc.com