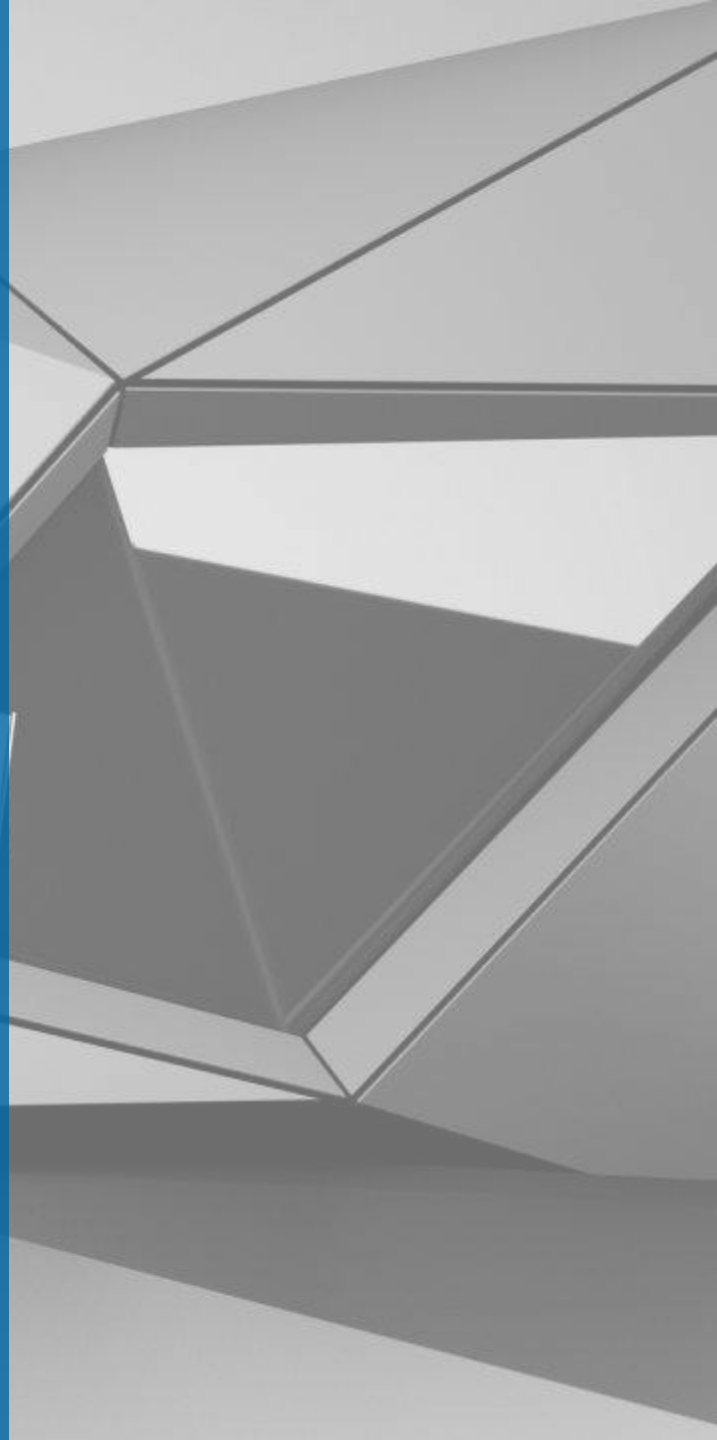
CREATe.org
Center *for* Responsible Enterprise And Trade

A New Approach to IP Protection and Safeguarding Trade Secrets

Pamela Passman
Center for Responsible Enterprise And Trade
(CREATe.org)
ppassman@create.org



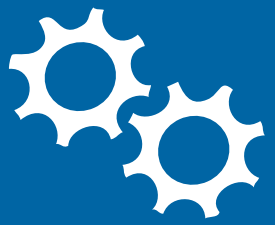
Center for Responsible Enterprise and Trade

CREATe.org

A **global NGO:**

- Focusing on **IP Protection** and **Anti-Corruption**
- Sharing **leading practices** based on insights from global companies, academics, organizations and think tanks

CREATe Leading Practices



Assessments and benchmarking to measure current processes/systems

Guidance and steps for improvement

Available in **English, Chinese, Spanish** and **Brazilian Portuguese**

CREATe.org
Center for Responsible Enterprise And Trade

Developments Beyond the EU: Asia, US and TPP

- **U.S. Pending Legislative Initiatives:** federal private civil action and seizure of goods
- **Trans Pacific Partnership Agreement (TPP):** leaked draft would require signatory countries to impose criminal penalties for trade secret misappropriation
- **Intensifying global competition** among industry players in Japan, Korea, Taiwan and China - leading to increased litigation

Trade Secret Theft: Increasing Global Threat

CREATE.org
Center for Responsible Enterprise And Trade

Key Findings

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

- Significant risk of IP infringement throughout the supply chain
  - Suppliers, business agents, partners equally pose IP risks
- Trade secret theft: greatest IP risk
  - 68% believe they have 'extensive risk' in this area
  - Only 36% rated their company compliance program effective
- Protecting IP: limit IP exposure among third parties
  - Tactics: splitting high-value IP among suppliers, limiting IP access
- Training is key to IP compliance
  - Focus is primarily on employees rather than 3rd parties

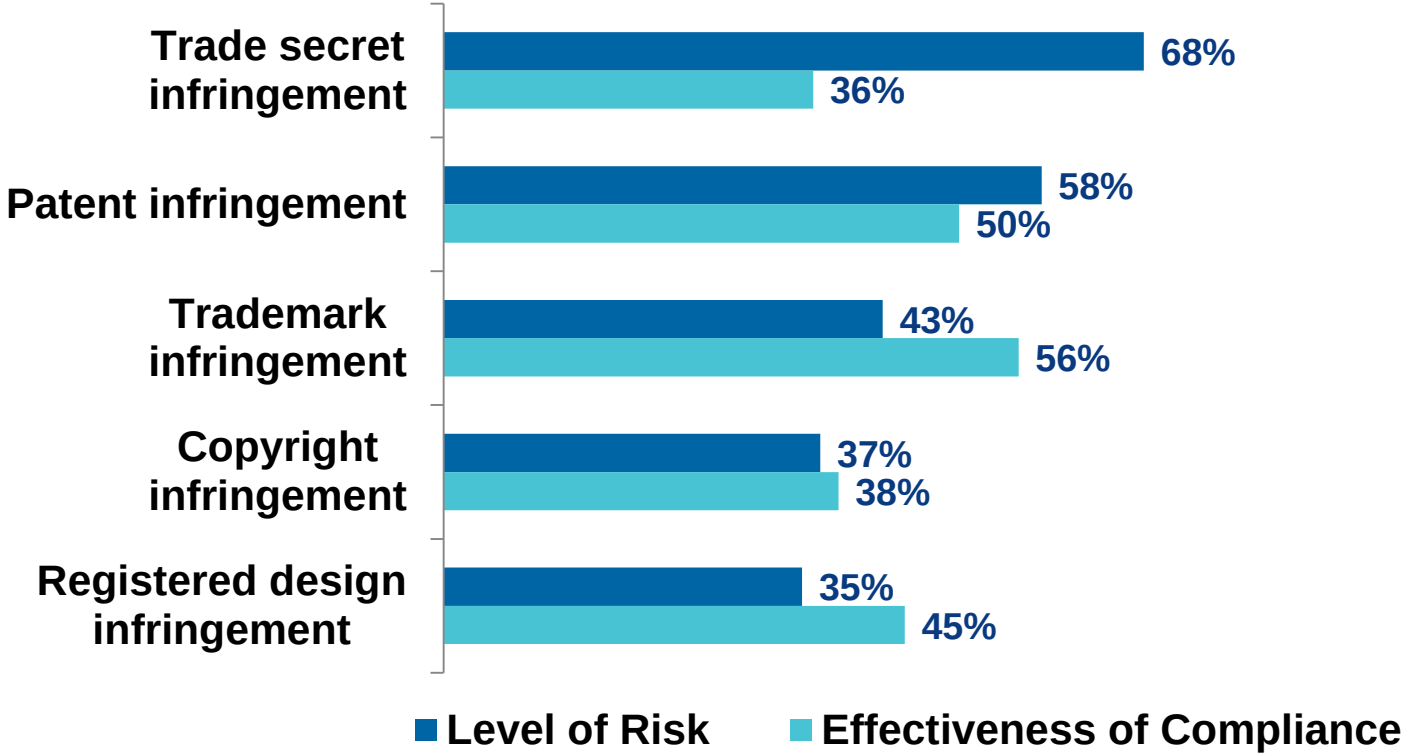
CREATE.org
Center for Responsible Enterprise And Trade

IP: Risk vs. Reality

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

Percentage of respondents who identified IP risk as an extensive risk and whether compliance program was very effective

Both measures rated 1 – 2 on a 5-point scale

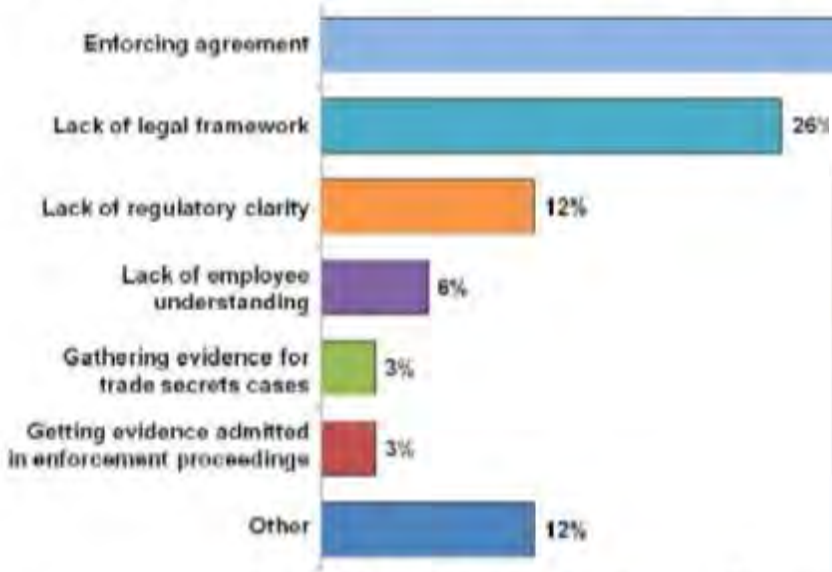


5. How much risk do you think there is of each of the following types of violations of your company's intellectual property when it engages third parties in emerging markets? 7. How effective do you think your company is in its efforts to prevent each of the following types of infringement of its intellectual property when it engages third parties in emerging markets?

CREATe.org
Center for Responsible Enterprise And Trade

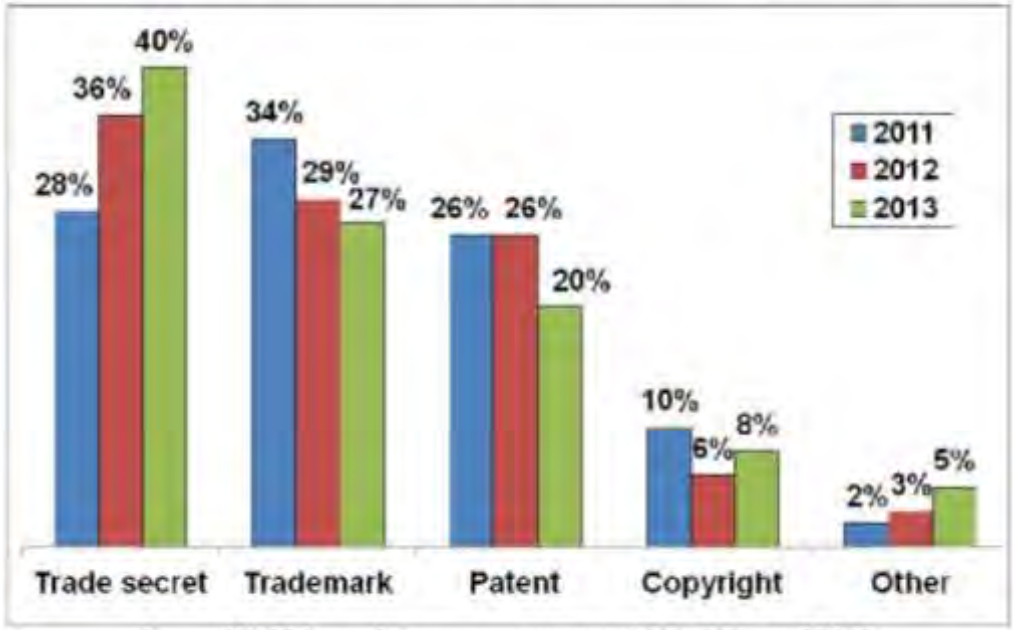
U.S. China Business Council Survey: Trade Secret Theft in China

Table 2: What Aspect of Trade Secret Protection in China Is of Greatest Concern?



Source: USCBC 2013 Member Company Survey

Table 1: Type of IP Infringement of Greatest Concern



Source: USCBC member company surveys (2011, 2012, and 2013)

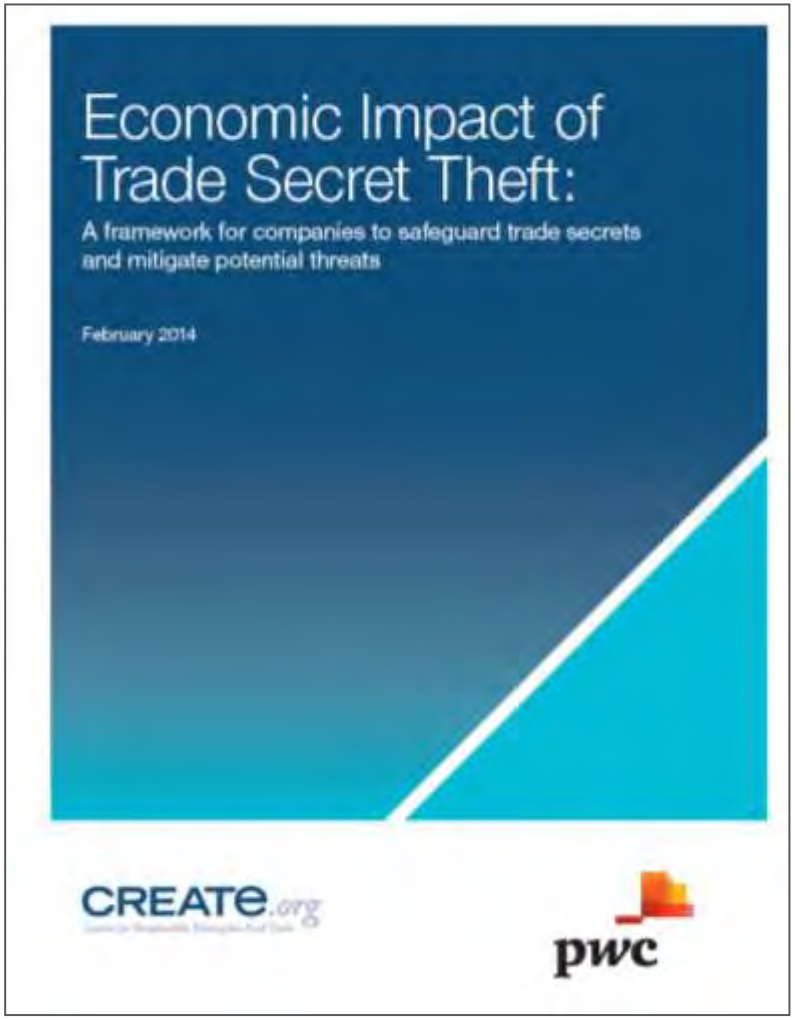
CREATE.org
Center for Responsible Enterprise And Trade

Framework for Safeguarding and Valuing Trade Secrets

CREATE.org
Center for Responsible Enterprise And Trade

CREATe – PwC Trade Secrets Report

- **The economic impact** of trade secret misappropriation;
- **An analysis of key threat actors**;
- **Three future scenarios** that envision trade secret protection outcomes in 10-15 years; and
- **A five-step framework to help companies assess and safeguard trade secrets**.



CREATe.org
Center for Responsible Enterprise And Trade

Framework: Objectives and Outputs

- ✓ **Consensus across business units** over definitions and criteria for determining IP that is a trade secret
- ✓ **Prioritized, ranked list of trade secrets** with location maps around the world
- ✓ **A clear repeatable process** for incorporating new innovations and trade secrets into the existing trade secrets list
- ✓ **Proven formula for assessing the cost** of trade secret theft at the individual level
- ✓ **Means to determine how to maximize the value** of protective measures to ensure the greatest return on security investment

CREATe – PwC Trade Secrets Report

- **Five-step framework to help companies assess and safeguard trade secrets**

Framework: Step 1 – Identify Trade Secrets

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

Framework: Step 2 – Assess Threat Actors

2 Threat Actor & Vulnerability Assessment

Assess threat and possible exposures

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

CREATE.org
Center for Responsible Enterprise And Trade

Step 3: Value Ranking of Trade Secrets

3 Relative Value Ranking

Trade secret value ranking analysis

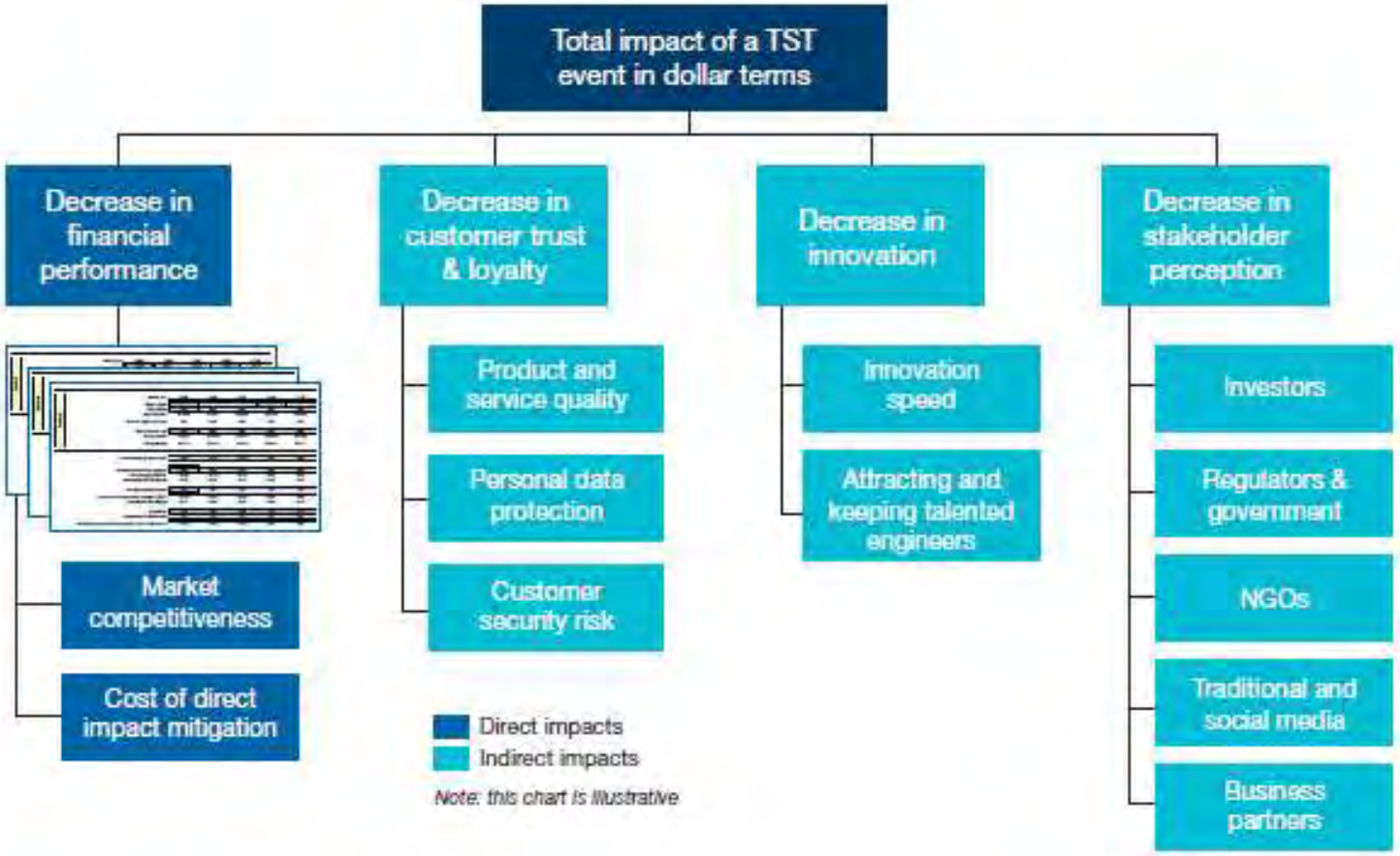
Establishing the Relative Value Ranking for Company Assets

	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

Framework: Step 4 - Economic Impact Analysis

4 Economic Impact Analysis

Analyze loss attributable to theft event



Framework: Step 5 – Secure Trade Secrets

Effective IP protection involves 8 categories:

Policies, Procedures & Records	IP Compliance Team	Scope & Quality of Risk Assessment	Management of Supply Chain
Security & Confidentiality Management	Training & Capacity Building	Monitoring & Measurement	Corrective Actions & Improvements

CREATe Leading Practices

Enhancing business processes to better safeguard IP, trade secrets and other proprietary information

CREATe.org
Center for Responsible Enterprise And Trade

The Trend: Supplementing Legal with a Management System Approach

Legal Approach

- Contract-driven
- Compliance is a silo in the legal department
- Typically reactive
- Seek legal remedy **if** problems are discovered

Management System Approach

- Builds awareness throughout the company
- Communicates clear expectations
- Preventative, proactive
- Builds on management systems used for other business operations

CREATe ▸ Leading Practices

For IP Protection

Measure

1 Self-Assessment

Online Q&A:

Measures maturity of systems in all categories

Rates maturity on a scale from 1 to 5

2 Independent Evaluation

CREATe expert evaluation:

Qualifies self-assessment

Reviews documentation

Generates verified score

Improve

3 Improvement Plan

Based on rating, company receives:

Improvement steps

Benchmarking report

CREATe.org
Center for Responsible Enterprise And Trade

CREATe.org

Center *for* Responsible Enterprise And Trade

Thank You

For more information about
CREATe Leading Practices,
please contact us at info@create.org