CREATe.org
Center *for* Responsible Enterprise And Trade

Leading Practices for Protecting Trade Secrets

Pamela Passman, President & CEO

Center for Responsible Enterprise And Trade
CREATe.org

Center for Responsible Enterprise And Trade

Mission

Global NGO dedicated to making leading practices in intellectual property (IP) protection and anti-corruption achievable for all companies

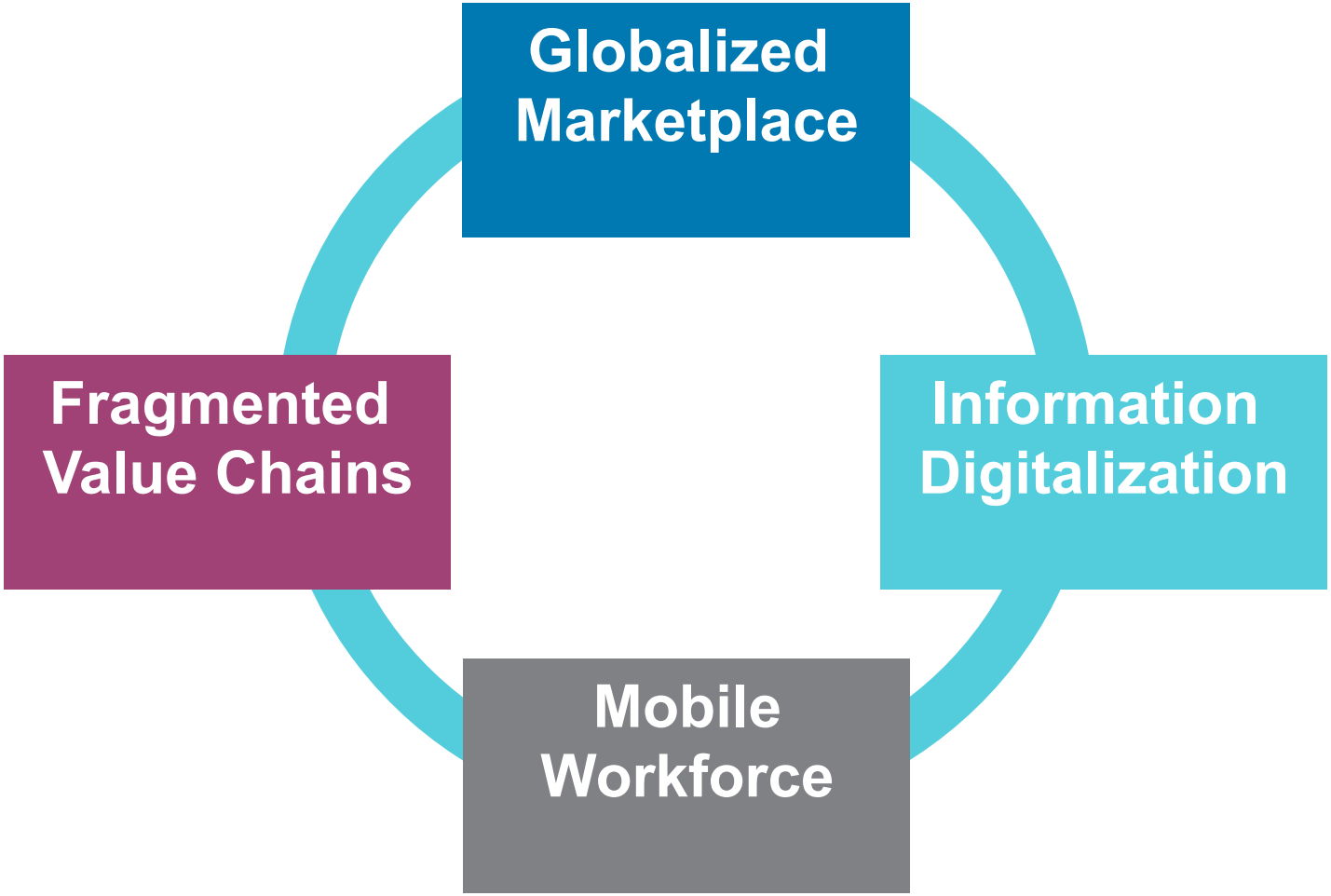
Global Reach

Working with companies in a range of industries in China, Brazil, India, Europe, Mexico, Japan, Singapore and the US

Services

CREATe Leading Practices: online assessments, evaluations, e-Learning, advisory

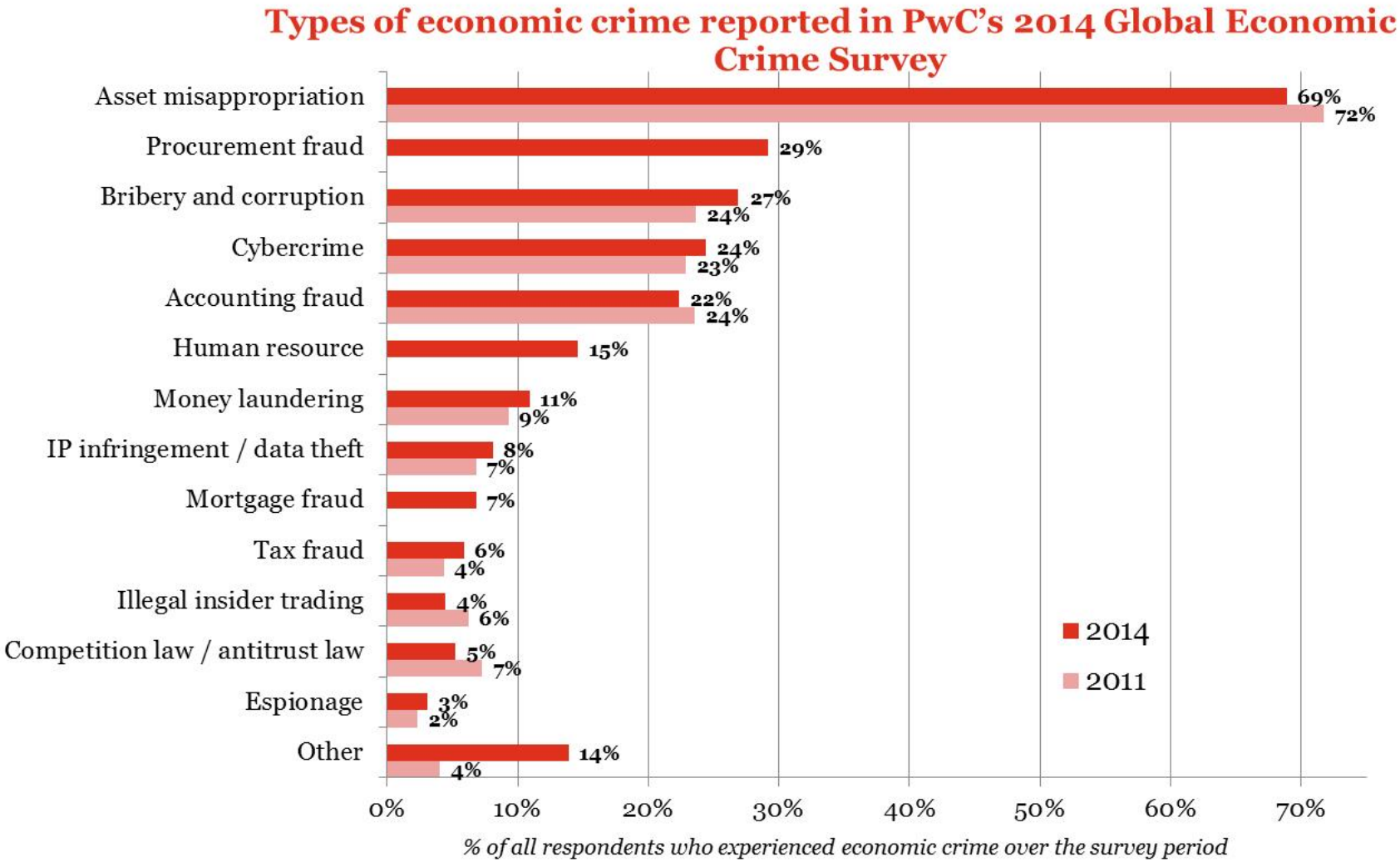
Why The Rise of IP and Trade Secret Theft?



Trade Secret Theft: A Major Threat Today

CREATE.org
Center for Responsible Enterprise And Trade

Putting Trade Secret Theft in Context

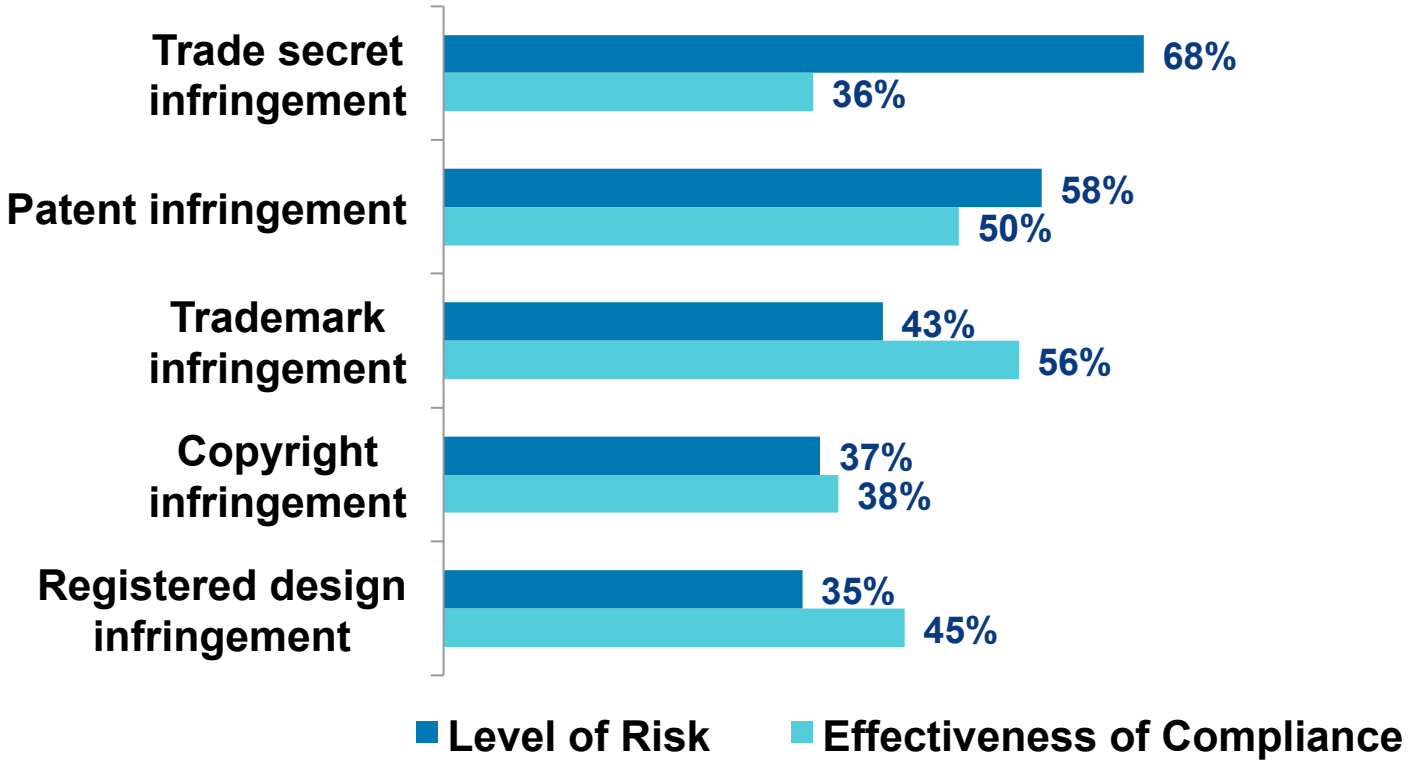


CREATE.org
Center for Responsible Enterprise And Trade

Trade Secret Protection: Risk vs. Reality

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



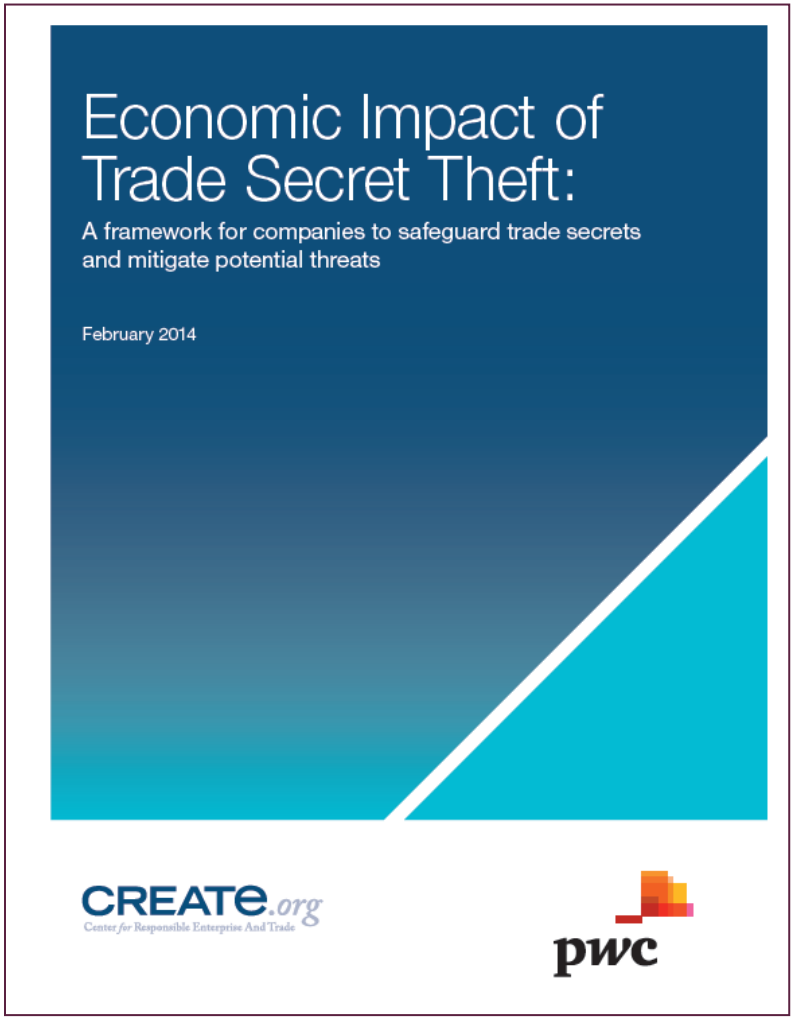
5. How much risk do you think there is of each of the following types of violations of your company's intellectual property when it engages third parties in emerging markets? 7. How effective do you think your company is in its efforts to prevent each of the following types of infringement of its intellectual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

CREATE.org
Center for Responsible Enterprise And Trade

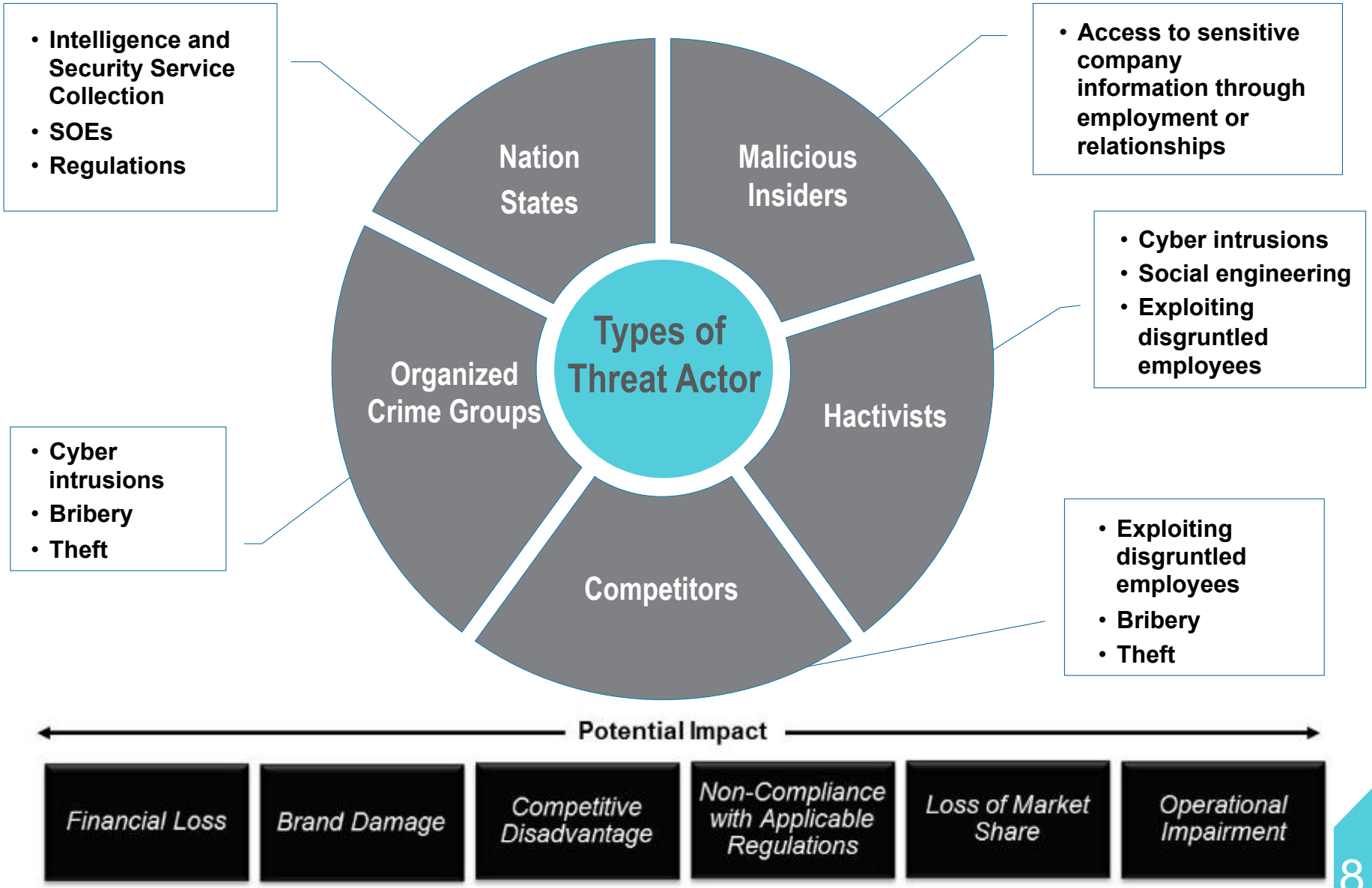
CREATe – PwC Trade Secrets Report

- **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**.

Available at www.CREATe.org



Who is Targeting Trade Secrets and How?



Malicious Insiders

Impact → Most common source of IP theft

Motivation → Ego, ideology, competition or financial gain

Access → Systems, records, source code, facilities

Connections → Malicious code, social engineering to exploit access

Red Flags → Activity changes with business events, employee departure

Another Insider: Supply Chain Partners

ft.com > reports >

The Connected Business

Home | World | Companies | Markets | Global Economy | Lex

Business Education | Entrepreneurship | Business Books | Business Travel | Recruitment | The Con

October 20, 2014 12:24 am

Hackers find suppliers are an easy way to target companies

Hannah Kuchler Author alerts

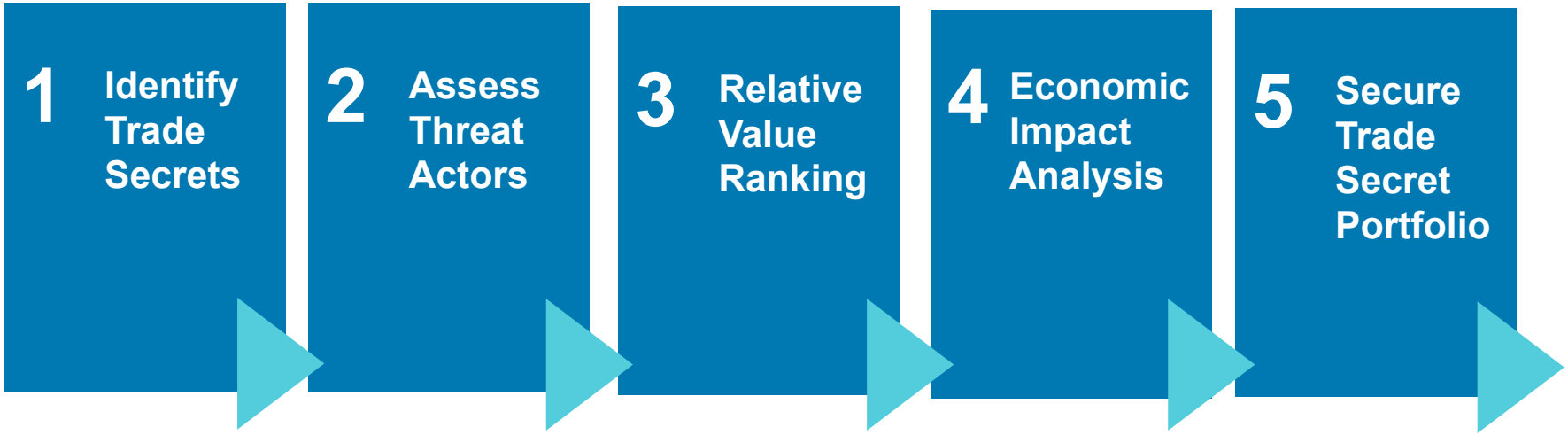
The windows may be bolted and the security gate locked, but security experts are warning that unless every other entrance and exit is secured, cyber criminals can still enter your company via your supply chain.

The risk of hackers entering a company's computer networks through a supplier – or even, the supplier of a supplier – has become a greater concern since the cyber attack on the US retailer Target late last year.

"The majority of the time, suppliers are the easiest way in"

Protecting Trade Secrets

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



Step 5: Securing and Protecting

5 Secure Trade Secret Portfolio

Enhance ability to secure assets

Categories of an Effective IP Protection Program

- 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

Optimizing Trade Secret Protection

- ✓ **Gain consensus across business units** over definitions and criteria for determining IP that is a trade secret
- ✓ **Create a prioritized, ranked list of trade secrets** with location maps around the world
- ✓ **Define a clear repeatable process** for incorporating new innovations and trade secrets into the existing trade secrets list
- ✓ **Use a proven formula for assessing the cost** of trade secret theft at the company level
- ✓ **Determine how to maximize the value** of protective measures to ensure the greatest return on security investment
- ✓ **Align people, processes and technology** to ensure that trade secrets are secret and protected

Additional Resources

CREATE.org
Center for Responsible Enterprise And Trade

CREATe ▸ Leading Practices

CREATe Leading Practices

3-step service

- Online Assessment
- Expert Evaluation
- Improvement Plan
  -200+pg Guides for Improving Programs

eLearning

15-minute courses

- Introduction to IP
- Trade Secret Protection
- Anti-Corruption

Advisory

Tailored assistance

- Workshops
- Implementation guidance
- Webinars

Additional CREATe Resources

Free Downloads
Available at www.CREATe.org

Protecting Intellectual Property Through Enterprise Risk Management (ERM)

Trade Secrets:

- CREATe-PwC Report/Framework
- Protecting Trade Secrets with Supply Chain Partners
- Model Policies: Trade Secrets

- Model IP Policies
- Health and Safety Risks of Counterfeits in the Supply Chain

CREATe.org
Center for Responsible Enterprise And Trade

CREATe.org

Center *for* Responsible Enterprise And Trade

Thank You

Pamela Passman
ppassman@CREATe.org

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