CREATe.org
Center for Responsible Enterprise And Trade

Quick Guide to Trade Secrets

An overview of trade secrets, the critical business information that provide companies with a competitive edge.

What are Trade Secrets?

Technical Information
Product formulas
Product designs
Manufacturing processes
Computer code

Business and Financial Information
Consumer preferences
Pricing information
Marketing and business plans

Read more: *Beginner's Guide to Trade Secrets*

When is it a Trade Secret?

Undisclosed
Valuable
Steps to keep it secret

Why Protect Trade Secrets?

Damage to companies from trade secret theft
Loss of competitive advantage
Damage to reputation
Financial penalties, legal costs and fines

Read more: *Beginner's Guide to Trade Secrets*

Where Does Trade Secret Theft Happen?

A Few Stats

3%
Value of Trade Theft as Related to U.S. GDP

The value of trade secret theft in the U.S. is approximately 1% – 3% of the gross domestic product (GDP) of the U.S. and other advanced industrial economies. (Source: CREATe – PwC: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats)

71%
Users with Access to Company Data

In a report by the independent Ponemon Institute, 71% of "end users" (employees on the system) said they have access to company data they should not be able to see, and 54% of them said that the access was frequent or very frequent. (Source: Ponemon Institute: Corporate Data: A Protected Asset or Ticking Timebomb?)

75%
Think Trade Secrets are Strategically Important

In an EC-sponsored survey of 537 businesses in Europe (EC, 2013), 75% of respondents ranked trade secrets as "strategically important to their company's growth, competitiveness and innovative performance." (Source: OECD: Approaches to Protection of Undisclosed Information (Trade Secrets))

Cases in Point

SolidWorks

An employee of an Indian company, Geometric Ltd., was given access to software source code owned by SolidWorks, a U.S.-based client. The employee was caught trying to sell the software code to SolidWorks' competitors yet it was not possible to sue him under Indian law since he technically had not stolen from his employer.

W.L. Gore and Associates

In April 2014, federal officials arrested Kwang Seoung Jeon at JFK airport, just before he was to fly his native South Korea. Jeon, who worked for the W.L. Gore and Associates, the Delaware textile company that invented Gore-Tex® allegedly was spotted printing out "book-sized" documents in the weeks before leaving the company. An investigation revealed that the chemical engineer had printed and downloaded hundreds of documents on a high-tech camouflage fabric the company was developing for military use.

American Superconductor

Massachusetts-based American Superconductor ("AMSC") makes wind turbines technology. Its top customer, China-based Sinovel Wind Group, paid an AMSC engineer to steal proprietary source code from AMSC's secure server in Austria. After Sinovel acquired the source code, it began turning away AMSC's shipments. Sinovel had previously provided more than 70% of AMSC's revenues, so the impact on AMSC was devastating. Its stock value plummeted 40% in a single day. AMSC's profits dropped; and it forced AMSC to cut jobs.

Who Steals Trade Secrets?

Greatest Threats

Organized Crime
Nation States
Malicious Insiders
Competitors
Hacktivists

Spotlight on: Malicious Insiders

- Most common source of IP Theft
- Motivation: Ego, ideology, competition or financial gain
- With access to: Systems, records, source code, facilities
- Connections with others: Malicious code, social engineering to exploit access
- Red flags: Activity changes with business events, employee departure

Read more: *Profile of a Malicious Insider*

How To Protect Trade Secrets

1. **Identify Trade Secrets** – Identify and categorize trade secrets
2. **Threat Actor & Vulnerability Assessment** – Assess threat and possible exposures
3. **Relative Value Ranking** – Trade secret value ranking analysis
4. **Economic Impact Analysis** – Analyze loss attributable to theft event
5. **Secure Trade Secret Portfolio** – Enhance ability to secure assets

Read more: *Companies: Five Steps to Protecting Trade Secrets*

Employees – If you are dealing with confidential information:

1. Put it away and don't email it
2. Guard it in public
3. Don't tell or give it to anyone
4. Put non-disclosure agreements in place
5. Use password protection
6. Control and track access

Read more: *Employees: Your Role in Keeping Trade Secrets "Secret"*

CREATe Resources:

- CREATe Leading Practices for Trade Secret Protection
- eLearning course: Protecting Trade Secrets
- CREATe – PwC: Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats
- Reasonable Steps to Protect Trade Secrets: Leading Practices in an Evolving Legal Landscape
- Trade Secret Theft: Managing the Growing Threat in Supply Chains
- Trade Secret Model Policies

External Resources:

- Secrets: Managing Information Assets in the Age of Cyberespionage
- OECD Report: Approaches to Protection of Undisclosed Information (Trade Secrets) (Including the Trade Secret Protection Index)
- Administration Strategy on Mitigating the Theft of U.S. Trade Secrets

CREATe Leading Practices: Learn more or try it now--free benchmarking!