

# WIPO SYMPOSIUM ON TRADE SECRETS AND INNOVATION

## Topic 5: Trade Secrets in the Value Chain

**World Intellectual Property Organization  
(WIPO), Tuesday, 24 May 2022**

**Dr. Richard L. Thurston, Esq.**

©RLT Global Consulting LLC, 2022



# Protecting Corporate Trade Secrets

## ❑ Trade Secrets are at the Core of Corporate Innovation.

- ❖ Increasingly, corporations are at **great risk arising from advancing technology developments** and the Post Computer Age (PCA), especially from borderless shared pools of information somewhere in the “Cloud” with Blockchain overlays.
- ❖ Corporate trade secrets are extremely important and valuable:
  - Estimated impact of trade secret theft is 1-3% of GDP of U.S. and other advanced countries.
  - Trade secret theft is widespread: It is estimated that 50% of employees who leave their jobs in the past year kept confidential corporate data, and plan to use it at a new job

## ❑ The Exact annual \$\$ loss for corporations cannot be calculated, but losses probably in the range of tens of billions of dollars, not including unmeasurable values for intangibles:

- ❖ Loss of competitive advantage;
- ❖ Loss of key elements of core technologies;
- ❖ Loss of company reputation;
- ❖ Loss of business opportunities;
- ❖ Loss of customers which would no longer trust your ability to protect their trade secrets;
- ❖ Loss of profitability, return on investment, etc.;
- ❖ Loss of shareholder value; and
- ❖ Loss of valuable/key personnel

# Protecting Corporate Trade Secrets

## □ Business espionage threats come from a myriad of sources, including:

- ❖ Governments;
- ❖ Corporations;
- ❖ Current and former employees;
- ❖ Customers, vendors, partners, and consultants;
- ❖ Academia and research institutions (through joint research projects, student access to corporate R&D; Ph.D. dissertations, etc.);
- ❖ Media;
- ❖ Information brokers, hedge funds and “consultant organizations” in what has been commonly referred to as "insider trading" – not just for stock market manipulation, but black market technology brokering; and
- ❖ Other.

# Protecting Corporate Trade Secrets

## □ **Examples of confidential information misappropriated from high-tech manufacturing include:**

- ❖ Complete process steps;
- ❖ Trade secrets underlying patent applications;
- ❖ Invention disclosures;
- ❖ Trial and error results (showing mistakes made);
- ❖ Information relating to tech transfer from mother facility to other facilities/plants;
- ❖ QR info;
- ❖ Employee names, organizational charts, contact information;
- ❖ Customer information, including customer product specs;
- ❖ Corporate policies and procedures;
- ❖ Facility/manufacturing plant designs and layouts; and
- ❖ Manufacturing equipment designs and layouts

# Protecting Corporate Trade Secrets, page 1

- ❑ All companies, whether small, medium or large, should create basic/tailored measures to protect their confidential and other proprietary information, including:
  - ❖ Establishing a robust ethics code;
  - ❖ Establishing customized trade secret policy and procedures;
  - ❖ Installing [sophisticated] IT systems and software with advanced monitoring and tracking capabilities;
  - ❖ Establishing and enforce strict controls over removable storage media;
  - ❖ Imposing [significant] restrictions on the ability of employees, vendors and suppliers to freely print, copy and distribute proprietary information;
  - ❖ Imposing controls over employee, vendor and supplier external Internet/web access
  - ❖ Proper classification and disposal of proprietary information; and
  - ❖ Creating strong NDA/confidentiality agreements, process and database with all customers, vendors, supplier and key employees

# Protecting Corporate Trade Secrets, page 2

## ❑ Tailored measures continued:

- ❖ Restricted access to proprietary information on a “need to know” basis only
- ❖ Effective employee on-boarding and off-boarding policy and procedures
- ❖ Enhanced training throughout the entire company, some of which should be mandatory for all employees, including an *e-Learning* course on trade secret protection:
  - Definition of trade secret (including its key elements and the relevant laws)
  - The worldwide threat of industrial espionage and the serious damages and impacts caused
  - What new employees should know about trade secrets
  - What departing employees should know about their trade secret obligations
  - The consequence of violating trade secret laws; and
  - Enhanced penalties for violation of corporate policies and procedures, including possible termination and criminal action by local authorities.
- ❖ Create and maintain an internal trade secret database.

# The Corporate Trade Secret Ecosystem

Key Strategic Elements:

Core sub-components:

*Note – Coloring is for Illustrative Purposes Only: Each Corporation Would Have Different Results Based on An Initial Internal Audit*

Color Key:

Well Developed

Basic structure , but not well-developed

Lacking or Immature

IP Development and Enforcement Elements	Trade Secret Management Elements	Contract Elements	Information Technology - Security Elements
Traditional Innovations and Inventions Processes and Procedures	Inventor/IP Assignments to Corporation	Traditional Contract Terms and Conditions	Basic IT Systems and protections
Patents	Publication review/public disclosure Policy	Licenses & Cross Licenses of Technologies and Traditional IP	Records retention
Traditional Trademarks	Simplification and consolidation of corporate policies/procedures	Traditional Contract Management Policies, Process and Procedures	"Clean room" R&D processes & procedures
Traditional Copyrights	Employee Hiring, Retention, Exit, post-employment, developing and retaining talent.	Confidentiality Agreements (NDAs)	Use of Third party IP and protection
Software	Restricted Access to technologies ("need to know")	Vendors and suppliers	Network & Database Access, storage and protection (i.e., encryption, passwords, computer forensics, etc.)
Traditional Trade Secrets	Employee Non-compete Agreements	Collaborative Arrangements with third parties and universities	Data mining including email & blog monitoring
Subsidiary and Affiliate Alignment	Creating a robust trade secret access (classification) system	Subsidiary and Affiliate Alignment	Inventory/Mapping intangible assets
Competitor IP Assessment	Creating a trade secret knowledge registry system (ie., IIPCC's IKR)	Digital/Smart Contracts, Blockchain and NFT Contract Platforms	Subsidiary and Affiliate Alignment
Traditional Data Mining	Subsidiary and Affiliate Alignment		
Digital Art, NFTs, Blockchain/Crypto, and Digitally-Enabled Platforms			
Traditional IP on the Digital Platform			

*NB – This chart presents a hypothetical framework of key elements that a corporation should incorporate into a company-wide trade secret program. It should be weaved into the very fabric of the company. Each element is interrelated with the others.*

# Protecting Corporate Trade Secrets

**THANK YOU**

FOR ANY QUESTIONS, PLEASE CONTACT ME AT:

Dr. Richard L. Thurston

RLT Global Consulting LLC

Email: [jingju2021@gmail.com](mailto:jingju2021@gmail.com)