



***Laying the Foundation:  
Managing Trade Secrets***

Lien Verbauwhede  
Consultant, SMEs Division  
World Intellectual Property Organization (WIPO)



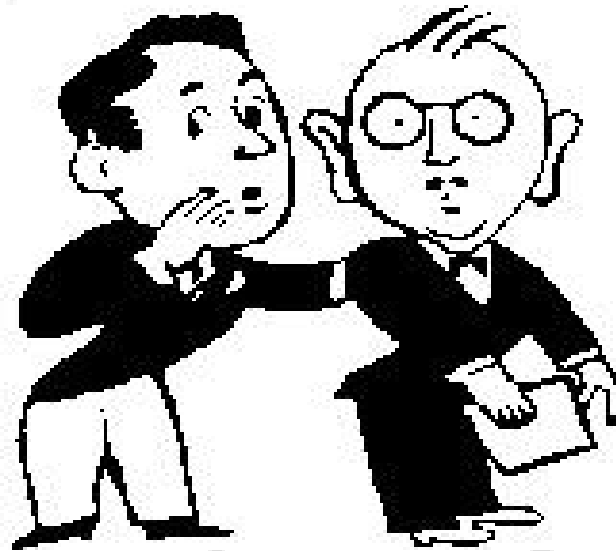
# **This presentation**

- **PART 1 - Outline**
  - Definition
  - Legal requirements
  - Rights
  - Enforcement
- **PART 2 - Trade secret or other IP?**
  - Advantages and disadvantages
  - When to choose for trade secret protection
- **PART 3 - Protection Strategies**



# PART 1

# WHAT ARE TRADE SECRETS ?





# What are trade secrets?

Broadly speaking,

- any **confidential** information
- which provides an enterprise with a **competitive edge**

can qualify as a trade secret



# Examples (1)

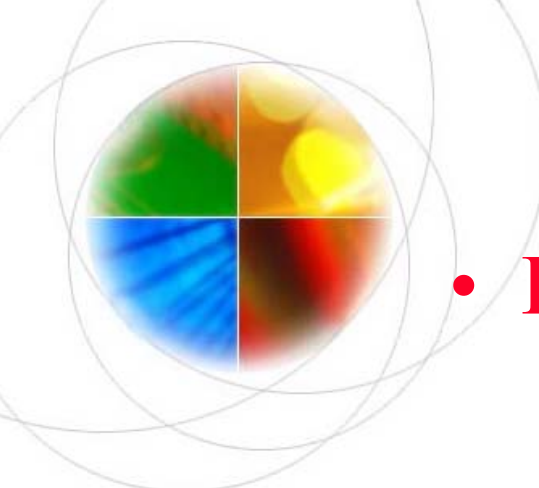
- **Technical and scientific information:**
  - formulas for producing products
  - technical composition of a product
  - manufacturing methods
  - designs, drawings, architectural plans, blueprints and maps
  - computer codes
  - test data, laboratory notebooks

## Examples (2)

- **Commercial information:**

- list of suppliers and clients
- customer buying preferences and requirements
- consumer profiles
- supplier arrangements
- marketing plan, business plan
- marketing strategy, business strategy, advertising strategy
- sales methods, distribution methods

# Examples (3)

- 
- **Financial information:**
    - internal cost structure
    - price lists
  - **Negative information:**
    - details of failed efforts to remedy problems in the manufacture of certain products
    - dead-ends in research
    - unsuccessful attempts to interest customers in purchasing a product



# What qualifies as a trade secret?

- Three essential legal requirements:
  - The information must be **secret** \*
  - It must have **commercial value** because it's secret
  - holder must have taken **reasonable steps** to keep it secret

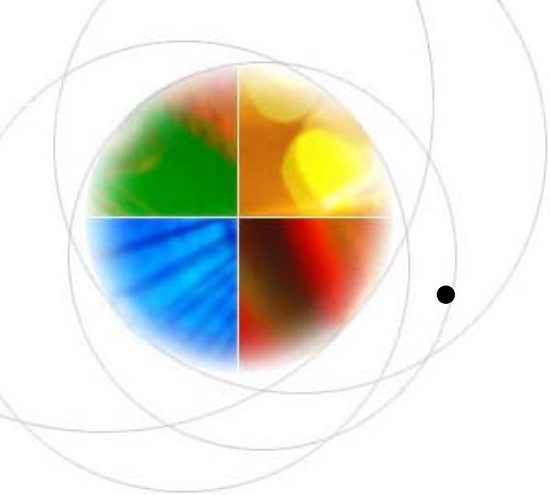
*\* “not generally known among or readily accessible to persons within the circles that normally deal with this kind of information”*





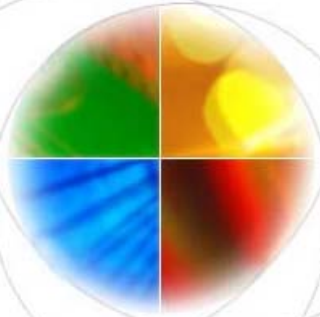
# What rights does the lawful owner of a trade secret have?

- Only protection against **improperly** acquiring, disclosing or using:
  - people who are automatically bound by duty of confidentiality (incl. employees);
  - people who have signed non-disclosure agreement;
  - people who acquire a trade secret through improper means (such as theft, industrial espionage, bribery);
  - people who knowingly obtain trade secrets from people who have no right to disclose them.



- One group of people cannot be stopped from using information under trade secret law:
  - people who discover the secret **independently**, without using illegal means or violating agreements or state law
    - e.g. consumer list
  - people who discover through **reverse engineering**
    - e.g. chocolate

→ **NO EXCLUSIVITY**



**What to do if someone steals  
or improperly discloses  
a trade secret?**



**Enforcement**



# Enforcement (1)

- Remedies

1. **compensation for damages** caused as a result of the misuse
2. Order to **stop the misusing**
3. **Precautionary impoundment** of the articles that include misused trade secrets, or the products that resulted of misusing



## Enforcement (2)

- To establish violation, the owner must be able to show :
  - infringement provides **competitive advantage**
  - **reasonable steps** to maintain secret
  - information obtained, used or disclosed in violation of the honest commercial practices (**misuse**)

## PART 2

# TRADE SECRETS OR OTHER IP?



*Weigh Your Alternatives*



# Trade Secrets vs Patents

- **No registration costs**  
but: costs to keep secret
- **No disclosure**  
but: practical need to disclose
- **Can last longer**  
but: limited to economic life  
+ risk to lose it if not secret
- **Fees registration + maintenance**
- **Disclosure**
- **Limited in time**  
generally: max 20 y



# Trade Secrets vs Patents

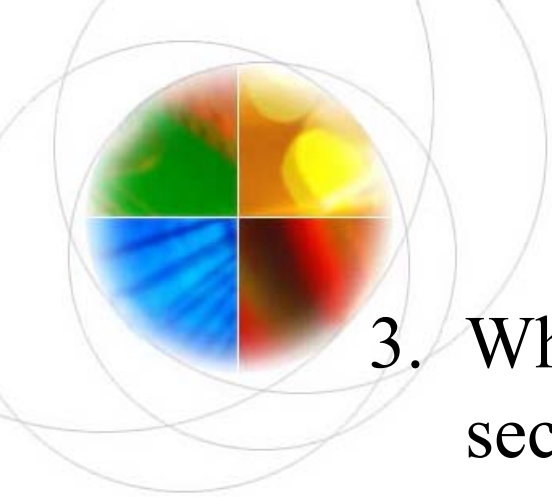
- Can protect info which is not protectable as patent
- Only protection against improper acquirem./ use
- More difficult to enforce  
unfair competition; some countries: no laws + irremediable
- Requirements  
new, non-obvious, useful
- Exclusive rights  
monopoly to exploit the invention
- “Power tool”





# TS or other protection?

- **Not suitable for all products, but should be considered along with the other forms of IP protection. Case-by-case basis.**
- **Trade secret protection may be advisable :**
  1. For inventions or manufacturing processes that do not meet the criteria for other protection
  2. When the trade secret is not considered to be of such great value to be deemed worth a P, UM, ID, TM



3. When it is likely that the information can be kept secret for a considerable period of time.
  - Coca-cola > 100y
  
4. When the secret relates to a manufacturing method or formula rather than to a product, as products would be more likely to be reverse engineered.
  - Mummification
  
5. When you have applied for other IP protection and are waiting for the P, UM, ID, TM to be granted.

# Example no. 1



- Decades ago, Coca-Cola decided to keep its soft drink formula a **secret**
- The formula is only know to a few people within the company
- Kept in the vault of a bank in Atlanta, Georgia
- Those who know the secret formula have signed non-disclosure agreements
- It is rumored that they are not allowed to travel together
- If it had patented its formula, the whole world would be making Coca-Cola

## Example no. 2



- **Patent** for stud and tube coupling system (the way bricks hold together)
- But: Today the patents have long expired and the company tries hard to keep out competitors by using **designs**, **trademarks** and **copyright**



# PART 3

## BUSINESS STRATEGIES TO HANDLE & PROTECT TRADE SECRETS





# **Loss of trade secrets - a growing problem (1)**

- **Why is this occurring?**
  - way we do business today (increased use of contractors, temporary workers, out-sourcing)
  - declining employee loyalty, more job changes
  - organized crime : discovered the money to be made in stealing high tech IP
  - storage facilities (CD-ROM, floppies, etc)
  - expanding use of wireless technology



# Loss of trade secrets - a growing problem (2)

- **Examples of outside threats**
  - burglaries by professional criminals targeting specific technology
  - attempted network attacks (hacks)
  - laptop computer theft: source code, product designs, marketing plans, customer lists
  - calls headhunters, presenting themselves as employee
  - corporate spies



# Loss of trade secrets - a growing problem (3)

- **Examples of inside threats**
  - **80% of information crimes < employees, contractors, trusted insiders!**
  - malicious destruction/erasure of R&D data by avenging employee
  - theft by former employee of business plans
  - ignorance





**What can be done?**



**10 basic protection strategies**





# 1. Identify trade secrets

## **Considerations in determining whether information is a trade secret:**

- Whether known outside the company
- Whether widely known by employees and others involved within the company
- Have measures been taken to guard its secrecy?



# 1. Identify trade secrets

- What is the value of the information for your company?
- What is the potential value for your competitors? (incl. neg. info)
- How much effort/money spent in collecting or developing it?
- How difficult would it be for others to acquire, collect or duplicate it?



## **2. Develop a protection policy**

### **Advantages of a written policy:**

- Transparency
- Clarity (how to identify and protect)
- How to reveal (in-house or to outsiders)
- Demonstrates commitment to protection → important in litigation



## 3. Educate employees

- **Prevent inadvertent disclosure** (ignorance)
- **Employment contract** :
  - Brief on protection expectations early
  - NDA/CA/NCA
  - obligations towards former employer!
- **Departing employees** :
  - exit interview, letter to new employer, treat fairly & compensate reasonably for patent work, further limit access to data



## 3. Educate employees

- **Educate and train:**
  - Copy of policy, intranet, periodic training & audit, etc.  
Make known that disclosure of a trade secret may result in termination and/or legal action
- **TS protection must be part of the enterprise culture**
  - Transform every employee into a potential security officer;
  - Every employee must contribute to maintain the security environment (e.g. anonymous security hotline)
- **Clear communication and repetition**
- **Monitor** compliance, prosecute violators



## 4. Restrict access

to only those persons having a  
**need to know**  
of the information

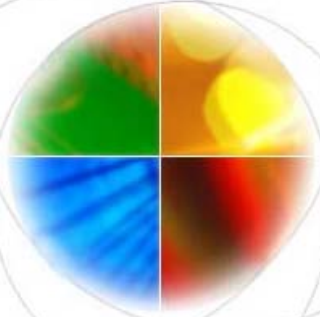
→ computer system should limit each employee's access to data actually utilized or needed for a transaction



## 5. Mark documents

- **Help employees recognize trade secrets**
  - prevents inadvertent disclosure
- **Uniform system of marking documents**
  - paper based
  - electronic (e.g. ‘confidential’ button on standard email screen)





## **6. Physically isolate and protect**

- Separate locked depository
- Authorization
- Access control
- Log of access (person, document reviewed)
- Surveillance of depository/company premises
- Shredding
- Oversight; audit trail



## 7. Maintain computer secrecy

- Authorization (password); access control
- Mark confidential or secret (legend pop, or before and after sensitive information)
- Physically isolate and lock: computer tapes, discs, other storage media
- E-mail; SMS messages
- Monitor remote access to servers
- Firewalls; anti-virus software; encryption
- Oversight; audit trail (for email: archive sent files)

## 8. Restrict public access to facilities

- Log and visitor's pass
- Accompany visitor
- Sometimes NDA/CA
- Visible to anyone walking through a company's premises (type of machinery, layout, physical handling of work in progress, etc)
- Overheard conversations
- Documents left in plain view
- Unattended waste baskets



## 9. Third parties

- Sharing for exploitation
- Consultants, financial advisors, computer programmers, web site host, designers, subcontractors, joint ventures, etc.
- Confidentiality agreement, non-disclosure agreement
- Limit access on need to know basis



## 10. Unsolicited submissions

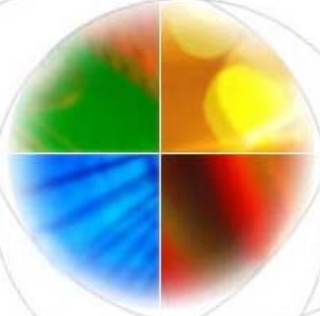
- Sharing for exploitation
- Consultants, financial advisors, computer programmers, web site host, designers, subcontractors, joint ventures, etc.
- Confidentiality agreement, nondisclosure agreement

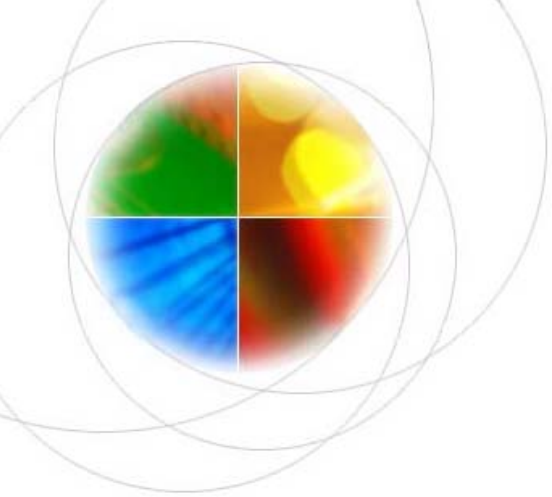


# Remember

- ➡ **No registration, but 3 requirements for legal protection**
- ➡ **Developing and maintaining TS program**
  - < **good business practice**
  - < **legal requirement for TS protection**

# Remember

- 
- ➡ No need for absolute secrecy, but ‘**reasonable** measures’ (e.g. DuPont)
  - ➡ Only legal protection against **dishonest** acquisition/disclosure/user in a manner
  - ➡ Consider alternative protection



WIPO's website:

**<http://www.wipo.int>**

WIPO's website for SMEs :

**<http://www.wipo.int/sme>**