František Bartes

Brno University of Technology, Faculty of Business and Management, Department of Economics, Kolejní 2906/4, 612 00 Brno, Czech Republic
email: bartes@fbm.vutbr.cz

Counter Competitive Intelligence Cycle

Abstract

The author's position is based on the well-known experience of Competitive Intelligence units that the classical cycle of Competitive Intelligence (management, collection, analysis and distribution) does not suit the defensive posture of Counter Competitive Intelligence. The reason why the offensive cycle of Competitive Intelligence does not fit Counter Competitive Intelligence is the fact that Counter Competitive Intelligence faces completely different tasks and therefore engages in different activities. Regrettably, professional literature dealing with the issues of Counter Competitive Intelligence touches upon this problem only marginally.

In this article, the author first defines the so-called "Basic Cycle of Counter Competitive Intelligence". He then proceeds to fill this basic cycle with all the essential activities that it should contain. The activities in the basic Counter Competitive Intelligence cycle are as follows: 1. Assignment. 2. Problem formulation and analysis. 3. Planning how to solve the problem. 4. Sourcing of data and information, including security measures. 5. Collecting essential data and information. 6. Processing collected data. 7. Information analysis. 8. Securing evidence. 9. Active intervention. 10. Evaluation and lessons learned. 11. Proposed measures. The author then outlines the appropriate content of activities in this basic Counter Competitive Intelligence cycle.

The article concludes with the individual activities of the basic Counter Competitive Intelligence cycle organized into the following 5-phase model of "Counter Competitive Intelligence Cycle": I. Planning and direction. II. Data collection. III. Analysis. IV. Action. V. Measures.

Key Words

competitive intelligence, counter competitive intelligence, intelligence cycle

JEL Classification: D80, G14, M15

Introduction

Any company with a position of prominence in a challenging market supports its strategic decision-making by gathering intelligence. This work is done by a Competitive Intelligence unit, see Bartes [1]. J. D. Rockefeller [11] expressed an opinion that "*the next best thing to knowing all about your own business is to know all about the other fellow's business*". In corporate practice, this means that success of an enterprise is always preceded by effective intelligence work, and failure is the consequence of either lack of intelligence or poor defensive performance of that unit. Counter Competitive Intelligence (CCI), being the defensive portion of the corporate Competitive Intelligence unit, then becomes very important. CCI's main task is to prevent the other participants in a competitive clash from obtaining our confidential information, especially the

information about the basis of our organizational system or our competitive advantage. American Society for Industrial Security (ASIS) cites the following four main consequences of not having a counterintelligence program [10]:

1. "Loss of competitive advantage.
2. Loss of market share.
3. Higher costs of research and development.
4. Increase in insurance premiums".

The intent of this article is to suggest potentially better approaches and/or conditions to attain a higher level of counterintelligence protection for a company in unforgiving competitive environment. This article was written using the methods of observation, analysis, synthesis, comparison and deduction.

1. Results

A survey of available literature about the work and procedures used by Competitive Intelligence personnel in safeguarding commercial secrets of corporations indicates that, aside from defining some rudimentary aspects of this type of protection, there is no routine or standard methodology. This is exemplified by publications authored by Fuld [5], Kahaner [6], Liebowitz [8], and particularly Carr [4], who describes the practices of 15 leading experts on Competitive Intelligence in the United States.

Our concept in protecting corporate trade secrets starts with a premise that such protection must be conceived as a unified system. Each of its subsystems listed below is equally important in protecting the company's trade secrets. It should be noted that the effectiveness of the whole system is determined by the strength of its weakest link, see Beranová, Martinovičová [3]. An overview of these subsystems is provided in Table 1.

Tab. 1 Subsystems ensuring protection of corporate trade secrets

	Name	Activity Description
1.	**Organizational**	a) Decision WHAT to keep secret and WHY. b) Categorization of buildings and structures. c) Monitoring the compliance with Trade Secret Protection Directive. d) Preparation of Company Security Policy.
2.	**Legal**	a) Legal protection of corporate intellectual property. b) Preparation of Trade Secret Protection Directive. c) Employment contracts with employees potentially exposed to company's trade secrets.
3.	**Personal**	a) Selection of employees potentially exposed to company's trade secrets. b) Periodic personnel training.
4.	**Physical**	a) Guarding of buildings, structures, etc. with human involvement. b) Mechanical security of those buildings and structures. c) Electronic security of buildings and structures.
5.	**Specific**	Company's counterintelligence protection

Source: prepared by author

To facilitate the management of activities implicit in these subsystems, they can be organized into the following three higher subsystems, namely:

1. Company security policy.
2. Company security protection.
3. Company counterintelligence protection.

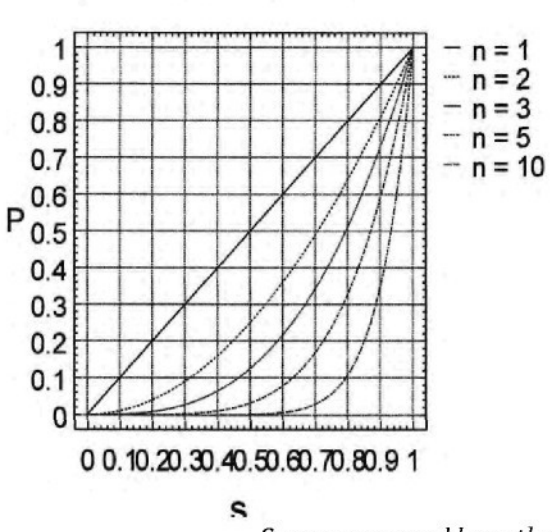
Given the intent of this article, it will discuss only the corporate counterintelligence protection with its fundamental objective to detect, in a timely manner, an intelligence breach or an industrial espionage attack, and to prevent a loss of classified information. Webster's New Collegiate Dictionary defines the leakage of information as *"information that has become known despite efforts at concealment".* The likelihood that information will be disclosed increases significantly with each individual carrier of that information. For these purposes, the following relationship can be derived from the probability theory:

$$P = s^n \tag{1}$$

where: P – probability that a given information will remain secret, s – reliability that the information will not be divulged by its carrier, n – number of information carriers.

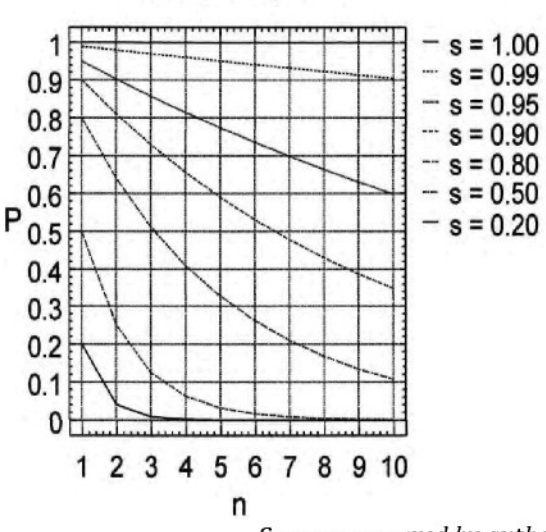
For simplicity, the above formula assumes the same reliability s for all information carriers. Plotting the probability P that given information will remain confidential due to reliability s of the information carrier for a varying number of information carriers produces diagram $P=P_{(s)}$ shown in Fig. 1. A graphic representation of the probability P that a certain information will remain confidential with n information carriers having different levels of reliability s is the function $P=P_{(n)}$ shown in Fig. 2.

Fig. 1 Graph of function $P=P_{(s)}$



Source: prepared by author

Fig. 2 Graph of function $P=P_{(n)}$



Source: prepared by author

These figures clearly show a sharp decline of probability that the information will be kept secret as a function of both the number of information carriers and their reliability. They indicate that the information is "*relatively safe*" when known to *only two* very reliable employees. The weakest link in the security of commercial trade secrets has been, is, and will always be, the human factor. Consequently, company employees, both current and former, represent the main risk. This issue was examined by Fuld [5], who offers his own formula for information leaks (see Table 2).

Tab. 2 Practical Application of the Information Leak Formula

Logic	Example	Rationale
Total number of employees.	60,000	Take into account all employees as each of them is in contact with the outside world.
25 % of the employees have frequent contacts.	15,000	A conservative estimate of those employees (in %) in frequent contact with their surroundings.
In a normal working day, each member of the 25 % group makes 5 telephone calls.	75,000 potential meetings or phone calls.	It resents a variety of opportunities when a leak may occur during a conversation
Assumption: only 1 % of these phone calls involve an active harmful information.	750 potentially damaging phone calls in one day.	Some leaks have an immediate effect on the company, others a delayed effect as a time bomb.
The number of leaks in a year with 250 working days.	187,500 potentially damaging leaks per year.	Assumption: no leak crossing.

Source: Fuld [5], modified by author

Based on the above, we can now define the concept of corporate counterintelligence protection as a "*specific corporate activity focusing on identification, detection and subsequent prevention of negative actions intending to uncover (steal) or otherwise compromise the trade secrets of our company. The effort has to be directed against the actions of our competitors as well as the negative actions of our own employees*", see Bartes [2]. Our basic precept in solving a given problem is the assumption that company's counterintelligence protection falls under intelligence services rather than corporate security. According to DeGenaro [11], this activity may be characterized as follows:

1. "Identification of critical information and activities.
2. Threat analysis.
3. Vulnerability analysis.
4. Risk assessment.
5. Selection of adequate countermeasures."

From the corporate practice of Competitive Intelligence units, it is obvious that even their defensive work can benefit from standardizing repetitive activities in a definite, periodically repeatable system. Such a system can be an intelligence cycle model that encompasses all basic activities which, in our opinion, a Counter Competitive Intelligence cycle should have. Table 3 provides a summary of these activities, under the tentative heading of Basic Counter Competitive Intelligence Cycle.

Tab. 3 Basic Counter Competitive Intelligence Cycle

No.	Name of Activity
1.	Assignment
2.	Problem formulation and analysis
3.	Planning how to solve the problem.
4.	Sourcing of data and information, including security measures
5.	Collecting essential data and information
6.	Processing collected data
7.	Information analysis
8.	Securing evidence
9.	Active intervention
10.	Evaluation and lessons learned
11.	Proposed measure

Source: prepared by author

The content of the individual activities listed in Table 3 is defined below.

1. Assignment

Among the defensive activities of Competitive Intelligence is the task of early recognition (identification) of an interest (attack), or even attempted industrial espionage, on our company by a Competitive Intelligence unit of another firm. It is therefore necessary to divide this initial activity of the basic Counter Competitive Intelligence cycle into two distinct functions:

1. **Internal function:** This function must begin with a decision of top corporate management to define the items that constitute the substance of trade secrets per par. 17-20 of commercial law. The Counter Competitive Intelligence has to respond by checking the function of the existing company system with regard to trade secret protection. Proposed at this point should be the different classification levels (WHO, WHAT, HOW, etc.), the information storage system, materials, as well as products and their record of manipulation (who, what, when, where, how, what, why). It is important to establish a feedback to know how the prerogatives and obligations are being carried out in the workplace. It is further necessary to define how the system functions, in its entirety and in each organizational element. These initial activities should also include an analysis of the system, its continual monitoring, and its development over time. The system must be fine-tuned to ensure that all occurrences deviating from the system's established norm are identified.
2. **External function:** The task of this external function is to give an early signal that the activities within the sphere of our corporate operations are being restricted, or the achievement of our strategic objectives threatened, or that an attempt has been made to compromise the ownership of our trade secrets. Sales Department, for example, must be able to define, in the external environment where it operates, what constitutes a disruption of our normal system functionality (see the description of internal functions). The same is true for other professional groups (relative to the external environment of our company, e.g. see Kocmanová, Dočekalová [7]).

2. Problem analysis and formulation

Should these internal and external signals be identified, the Counter Competitive Intelligence unit must be able to:

1. determine (find out) WHO, WHAT, HOW etc.
2. ascertain how the competing company works (in principle) and verify that its activities in our sphere of interest have nothing to do with breaches of discipline by our employees. The conclusion might be that it deploys very sophisticated methods of Competitive Intelligence, or conversely that it does not even have a CI unit and the result of its activity is corresponds to its creative potential, etc.

On the basis of this analysis, we can articulate our problem as follows:

1. our own system is failing (there are leaks of classified information, or the system produces symptoms that are readily identifiable and readable by the Competitive Intelligence unit of a competing firm),
2. external environment (a competing firm) is getting the upper hand and wants to take a greater advantage of the competitive space that the situation offers.

3. Planning how to solve the problem

The crux of the problem lies in the fact that functionality of our system is in jeopardy. Now the situation has to be assessed from an economic as well as personal viewpoint, in the following manner:

1. I have to re-evaluate the internal company system with regard to its own function and its level of trade secret protection.
2. Based on the internal system changes, it is necessary to institute appropriate changes and security measures in the external system of trade secret protection.

4. Sourcing of data and information, including security measures

We must establish a new organizational structure and function in the company, re-evaluate the scope of protected information in all its sections, impose new restrictions on the sharing of classified information. It is necessary to designate what needs to be "watched" at individual workstations. The system has to be set up so that we know that what was instituted is being followed. It is in essence a system of reports and means of monitoring the system to ascertain that the new system functions as required.

5. Collecting essential data and information

From the perspective of a new organizational structure, we need to establish what tasks will the employees perform and what will be the outputs. These outputs, in a suitable form, will be submitted to the Counter Competitive Intelligence unit.

6. Processing the collected data

A system configured as described generates a large amount of information from both the internal and the external function. This information can be categorized as

1. official information – coming from a function of corporate system
2. specific information – coming from specific sources.

7. Information analysis

All processed information must be analyzed. The output should be usable information, i.e. intelligence. The activity should conclude with an assessment how serious are the established facts. It is also necessary to evaluate the resources and methods that Competitive Intelligence units of competing companies used in their offensive.

8. Securing evidence

The collected evidence should match the gravity of the detected actions. Taking into account the preceding analysis, it is necessary to determine whether some of the collected and analyzed reports could serve as evidence.

9. Active intervention

The purpose of an intervention is to prevent a negative activity, or at least put a stop to it. The nature of an active intervention depends on the specific pieces of evidence that can be used. One has to consider WHAT, HOW, and TO WHAT EXTENT is an item useable. If at least some are usable, it is possible to deal with such a conduct officially. However, if an official use of the evidence is undesirable due to source protection concerns, then it is necessary to take appropriate organizational measures so that the negative activities would not continue.

10. Evaluation and lessons learned

Every concrete action should be followed by an assessment how effectively our system works. WHAT needs improvement, WHAT was done well, WHAT works as expected, WHAT should be altered, etc. Concrete action refers to cases identified by an alert that the system function was somehow compromised plus the cases uncovered during the regular checks performed to verify the activity level of our system.

11. Measures proposed

The evaluation performed in No. 10, should be put on the company project list and implemented in the shortest possible time.

2. Discussion

The foregoing activities of the Basic Counter Competitive Intelligence can be grouped by their linkage and similarity into the following five phases of the Counter Competitive Intelligence Cycle, see Table 4.

Tab. 4 Counter Competitive Intelligence Cycle

Phase of CCI Cycle		Activities of the Basic CCI Cycle
I.	Planning and direction	Contains activities 1; 2 and 3
II.	Data collection	Contains activities 4 and 5
III	Analysis	Contains activities 6; 7 and 8
IV	Action	Contains activity 9
V.	Measures	Contains activities 10 and 11

Source: prepared by author

As a practical matter, a Counter Competitive Intelligence unit can organize the above activities of the Basic CCI Cycle around the habits, possibilities, or abilities into a four-phase Counter Competitive Intelligence Cycle model. In that case, the phases of Data Collection and Analysis merge into one.

The five-phase model of the Counter Competitive Intelligence cycle described above was implemented in four companies. The introduction of this model took, on average, a period of three months. The implementation required the addition of one person to Competitive Intelligence. The results began to show in the next 4 – 6 months after putting the CCI model into practice. During that time, it was already possible to collect and analyze much information about the competition trying to acquire certain parts of trade secrets in those companies. Thereafter, it was possible to evaluate specific intelligence attacks of rival companies and, on this basis, adopt appropriate countermeasures. These countermeasures greatly enhanced the effective protection of our corporate trade secrets.

Conclusion

A well known fact, born out by many practical cases, is that the harder the competitive struggle in tough markets, the more ideas are stolen. We should keep in mind that this domain called "industrial espionage" cannot be totally eradicated since competition cannot be expunged in market economy nor egalitarian conditions imposed on all players in the economic arena by taking away the trade secrets of corporations. This means that as long as there are trade secrets helping the company achieve better economic results in the marketplace, the phenomenon of industrial espionage is bound to exist!

In the current corporate practice, the existence of industrial espionage is complemented by a perfectly legal and highly sophisticated endeavor of Competitive Intelligence units of competing companies. Our businesses need to learn how to defend themselves against that activity, too, because according to [11]: *"an attacker may be able to hide part*

of its actions all the time, or all of its actions part of the time, but it can never conceal all of its actions all the time".

Acknowledgements

This article was written as part of Faculty of Business Research Task No. FP-S-13-2052 "Microeconomic and macroeconomic principles and their impact on the behavior of households and firms."

References

[1] BARTES, F. Competitive intelligence – tool obtaining specific basic for strategic decision making TOP management firm. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis,* 2010, **58**(6): 43 – 50. ISSN 1211-8516.

[2] BARTES, F. *Competitive Intelligence. Základ pro strategické rozhodování podniku.* Ostrava: Key Publishing, 2012. ISBN 978-80-7418-113-9.

[3] BERANOVÁ, M., MARTINOVIČOVÁ, D. Application of the theory of decision making under risk and uncertainty at modelling of costs. *Agricultural Economics,* 2010, **56**(5): 201 – 208. ISSN 0139-570X.

[4] CARR, M. M. *Super Searchers on Competitive Intelligence.* New Jersey: Reva Basch, 2003. ISBN 0-910965-64-1.

[5] FULD, L. M. *The New Competitor Intelligence.* New York: John Wiley & Sons, 1995. ISBN 0-471-58509-2.

[6] KAHANER, L. *Competitive Intelligence.* New York: Simon & Schuster, 1997. ISBN 978-0-684-84404-6.

[7] KOCMANOVÁ, A., DOČEKALOVÁ, M. Environmental, Social, and Economic Performance and Sustainability in SMEs. In KOCOUREK, A. (ed.) *Proceedings of the 10th International Conference Liberec Economic Forum 2011.* Liberec: Technical University of Liberec, 2011, pp. 242 – 251. ISBN 978-80-7372-755-0.

[8] LIEBOWITZ, J. *Strategic Intelligence.* New York: Taylor & Francis Group, 2006. ISBN 0-8493-9868-1.

[9] MARTINOVIČOVÁ, D., BERANOVÁ, M., POLÁK, J., DRDLA, M. Teoretické aspekty kategorizace rizik. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis,* 2010, **57**(3): 131 – 136. ISSN 1211-8516.

[10] *American Society for Industrial Security (ASIS)* [online]. [cit. 2013-03-30]. Available from WWW: <http://www.asisonline.org/>

[11] *DeGenaro & Associates Incorporated* [online]. [cit. 2013-03-30]. Available from WWW: <http://www.biz-intel.com/>