ICEB 2009 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-4-2009

Sharing Competitive Intelligence, Securing Company Knowledge – A Framework

Ilona Ilvonen

Vilma Vuori

SHARING COMPETITIVE INTELLIGENCE, SECURING COMPANY KNOWLEDGE – A FRAMEWORK

Ilona Ilvonen[1] and Vilma Vuori[2]
Department of Business Information Management and Logistics
Tampere University of Technology, Finland
[1]ilona.ilvonen@tut.fi; [2]vilma.vuori@tut.fi

Abstract

This paper discusses the recognition of critical knowledge residing in companies. Company employees are important sources of competitive knowledge. At the same time the employees have a key role in securing critical knowledge in the company. A framework for recognizing critical knowledge is presented to work for both competitive intelligence and knowledge security perspectives. Employee awareness is essential to both of these perspectives, and the framework is intended to be used in building this awareness.

Keywords: Competitive Intelligence, Competitive Knowledge, Knowledge Security, Knowledge Sharing

Introduction

Competitive intelligence is a process that provides decision-makers with actionable information about what is happening in a company's business environment. Understanding and anticipating competitors' actions, possible changes in legislation or launch of a new competing product is essential for the company to maintain and improve its competitive position. A recent trend in competitive intelligence is shifting from analyst-centered competitive intelligence unit serving only the top management into involving all employees and in some cases even external partners, such as suppliers or customers, to participate in competitive intelligence activities (see e.g. [1], [2]).

Employees are seen not only as valuable sources of competitive information but also having an important role in refining that information. When information regarding competitive environment is processed in employees' head to have a concrete meaning in the company's context it is simultaneously refined into more valuable and usable form; competitive knowledge [3].

Companies aim to the best possible use of competitive knowledge. There are many mechanisms that aim to efficient knowledge sharing within a company. Competitive intelligence is an area where the smallest bits of knowledge about the operations and plans of competitors should be gathered together in order to construct a good overall picture of the competitive environment of a company. Knowing what kind of knowledge is worth sharing within the company is essential for the competitive intelligence process to work efficiently.

When a company tries to protect the competitive position it has, it is essential to keep important knowledge inside the company. Information security processes are built to prevent information from leaking outside. What these processes do not protect as easily is knowledge that resides in the heads of employees. Empowering employees to participate in competitive intelligence efforts may provide the company with better understanding about competitive issues, but it also causes more risks for the company's information security. How people behave, what they discuss and with whom should be planned and controlled, at least to some extent, so that even the smallest bits of knowledge that might be useful for competitors are kept safe.

Sharing competitive intelligence and keeping company knowledge secure are the two sides of the same medal: important knowledge. The key for success of both activities is the awareness of employees about what knowledge is valuable to the operations of a company. This paper draws on this common factor to build a framework on how to recognize important knowledge, and how to build awareness of it.

Competitive intelligence

A company's strategy and operations are based on its view on the surrounding world. The view is constructed on the understanding the company has of its surroundings, what is going on and why. Companies apply different kinds of intelligence activities to provide decision makers information to help them build a solid understanding of the prevailing situation and what might be lying ahead. Competitive intelligence is one approach for doing this. Competitive intelligence is continuous scanning of the environment, gathering and linking bits and pieces of information and analyzing them to provide insights to back up decisions that further the company's business goals [4], [5], [6]. Such external issues as future economic situation, competitors' actions, customer needs and consumer trends, changes in legislation etc. are in the focus of competitive intelligence.

Competitive intelligence can be described as a process which, according to several authors (see e.g. [7], [8], [9], [10], [11], [12]), typically consists of the following phases:

- identifying what information is needed in the organization,
- gathering information from multiple sources according to the needs,
- processing and analyzing information by combining it with existing knowledge and applying suitable analysis methods,
- disseminating and sharing information in form of analyses, presentations, reports etc. and storing it in databases or other suitable places, and
- using the information to form decisions that steer the organization towards its goals.

The textbook example of how to do competitive intelligence most efficiently, that has been promoted for last decade, is a centralized, professional and organized competitive intelligence unit (see e.g. [13], [14], [2]). The unit usually consists of a competitive intelligence manager and analysts, whose responsibility it is to provide the needed information to decision makers at the right time in a suitable form. In other words, carrying out the competitive intelligence process and serving the needs of information users. Regardless of the advantages of such an efficiently organized unit, it does not suit every company and all situations. Alternative approaches, such as competitive intelligence networks, have started to gain more attention in recent years. Some companies do very well even without any organized competitive intelligence gathering.

During the last few decades competitive intelligence has evolved from informal and tactically oriented data-gathering into formal competitive intelligence units serving strategic decision making as described above [14]. The next evolutional step of competitive intelligence is that it is no longer the prerogative of the top management practiced by competitive intelligence experts. Instead, competitive intelligence is demystifying, decentralizing and shifting “from serving the few to empowering the many” [2]. The new stage of competitive intelligence emphasizes the value and significance of human input in the competitive intelligence process over information systems and engages employees in the process.

Employees as competitive knowledge assets

The sources of ccompetitive intelligence are various: from personal human contacts to the internet and data bases. The most used sources are often the explicit ones, such as reports from a database, news service feeds or consultant analyses, because due to their definite form they are easier to reach and utilize. Nevertheless the sources more difficult to reach are often more advantageous and human sources are especially valued (see e.g. [15], [8], [16], [17]). For example, using a search engine to find information from the Internet is cheap, quick and brings abundant amount of answers related to the used search terms. However, the search results, though numerous, may not be very accurate or useful in any way. In addition, information obtained from a source available for everyone, such as a public database, does not bring much of an advantage to a company, because the competitors can as easily get the same information from the same source just as easily and fast. Therefore unique sources that possess critical knowledge are of great value.

A company’s own employees are important competitive knowledge assets, and Collins [8] even names them as the biggest intelligence asset of a company. They may have interesting information about competitors, customers and the market situation and they can provide in depth explanations and interpretations to information [16], [18], [19]. This refines information into knowledge that has more value to its holder and receiver. Vitt et al. [12] note, that human input is the key ingredient in creating knowledge, because knowledge cannot be generated through mere technology. Employees can therefore have a valuable role in piecing together a puzzle that reveals a clearer picture of what is going on in a company’s business environment: they create and posses competitive knowledge.

The best source of potential competitive advantage is in knowledge that makes a difference, and is obtained and acted upon before competitors get their hands on it. A company has the best and possibly exclusive access to its employees’ competitive knowledge. The employees can be made aware of the company’s information needs and thus harnessed to be active information gatherers, interpreters and sharers.

Engaging employees in the competitive intelligence process is recognized to be worthwhile, even though not always an easy task. Fuld, Bernhardt and Herring state that the potential of employees as information sources has been underutilized due to a lack of communication and coordination [20]. Employees do not know that the knowledge they possess might be of value to the company or there is no coordination or medium to share knowledge to others in the company.

However, it must also be pointed out, that not all knowledge employees have is relevant for competitive intelligence purposes, and therefore it is important to identify and communicate what kind of knowledge is interesting and indispensable for the company and should therefore be shared. On the other hand, employees possessing so much important knowledge to their own company can also cause risks.

Knowledge security

Security as a state is often defined as a lack of threat toward an object [21]. When an object is physical in nature, the threats can be more easily identified. A house can be threatened by a flood, or trees falling down. Money transported from a supermarket to the bank is threatened by robbers. The threats that an immaterial object faces are more difficult to recognize. Knowledge is highly immaterial in nature, and thus it is difficult to name all the threats toward it. Despite this difficulty, knowledge, as an important asset to a company, needs to be secured.

When planning the securing of an object it is important to recognize all the threats that face it. At this point discussion on what is a threat is essential. A threat is the consequences of an unwanted event. An example of a threat to knowledge is the unveiling of a plan to publish a new product. This threat can realize itself for example through casual conversation in the wrong place or by an email sent to the wrong recipient. One way to analyze and compare threats is to assign a value to them. The most informative way to do this is to estimate a monetary value to the threat. In the case of physical objects this is fairly straightforward: if a building is damaged, the costs of repair can be estimated quite accurately. In the case of immaterial objects such as knowledge the task is not as easy. How much will the company lose money, if a competitor can react to a product launch early? What is the value of product development knowledge? Even though the task seems impossible, even crude monetary estimates give something to work with (see e.g. [22]).

The estimate of the size of the threat does not usually provide enough information about the threats in order to make decisions on what threats to address and how. As all actions of a company, also security needs to be reasoned and prioritized. Therefore the concept of risk is more familiar to many decision makers. Risk can be defined in a simple formula:

Risk = threat * probability

Although the usefulness and reasonability of the whole concept of risk can be challenged [23], it is a useful tool when security investment decisions are done and security measures planned. One way to use the concept of risk is to calculate a monetary risk value to every identified threat. In the case of knowledge this leads to a crude estimate of monetary consequence being multiplied by a crude estimate of probability. As such, the risk figures are not very trustworthy and provide little value to the decision maker. A simpler way is to assess both the probability and the monetary consequences in a three-step scale as illustrated in Table 1.

Table 1. **The risk matrix.**

Consequences Probability	Mild	Moderate	Severe
Strong	Moderate risk, actions need to be considered	High risk, needs to be addressed	Critical risk, must be addressed
Moderate	Moderate risk, actions need to be considered	High risk, needs to be addressed	High risk, needs to be addressed
Weak	Small risk, no actions are urgent	Moderate risk, actions need to be considered	High risk, needs to be addressed

The risk matrix gives the security planner a tool to assess different threats and to select which ones to address first [24]. There are basically two ways to lower a risk: by reducing the consequences or by lowering the probability. In the case of critical or high risks, both aspects need to be done. How this is done depends on the threat and the asset that needs to be protected.

As risk assessment tools can be helpful in reasoning the security measures, they don’t provide with the actual solutions to how to protect important assets. When it comes to knowledge, securing it can be as difficult as it is to assess the risk facing it. Knowledge is immaterial, and mostly bound to people. Thus securing knowledge requires affecting the way people behave.

It is said that 80 % of information security risks are caused by people [25]. As knowledge can here be seen as a sub-section of information, it is fairly safe to state that nearly every threat to knowledge is caused by people. Human error has a remarkably big role in these threats. From the risk management perspective the consequences of human error is hard to lower. Some technical limitations for example to the kind and size of documents allowed to be attached to emails can be set. However, there is no technical way to limit the subjects an employee chooses to discuss for example in a fair or seminar, nor to limit the places he/she decides to take an important business call. Awareness of threats by every employee is the only way to affect both the consequences and the probability of a threat.

Knowledge security as a concept refers to the ability of a company to protect its intellectual assets [26]. Key ways to protect knowledge are to promote awareness of threats to knowledge, and to limit the amount of people that have access to critical knowledge. Not only need the employees be aware of threats that face critical knowledge, they need to be able to decide what knowledge is critical, and what they are to do with it in different situations.

Critical knowledge

Classifying critical knowledge

When the previous two sections of this paper are examined, some similar characteristics can be seen. Both competitive intelligence and knowledge security efforts rely on the ability of employees to recognize important knowledge, and act accordingly. In knowledge security the necessary action with critical knowledge is to keep it safe. In competitive intelligence the necessary action is to share this knowledge with the right people.

These similarities lead to a conclusion, that both the fields of competitive intelligence and security are to be considered when business critical knowledge is handled in an organization. The big challenge from both viewpoints is how to recognize what knowledge is critical to the company.

The information a company considers critical for its success varies depending on the company, situation and context. The company's game plan – its strategy – also has an impact on the information needs. If the aim is to be the market leader, the company making the bold decisions and growing by buying out competing companies, the need of information concerning the production capability and profitability of a competitor's different manufacturing sites is far greater than for a company which lives by the rules of merely keeping the status quo [27], [28]. In addition, in the case of a highly competitive strategy the value of getting critical information to use before others increases. Therefore it is important to have access to information assets that competitors do not have.

Hannula and Pirttimäki [29] have examined business information needs in a form of a three-dimensional cube. The dimensions are information subject (internal-external), information source (internal-external) and information type (qualitative-quantitative). Using Hannula and Pirttimäki's [29] categorization of business information a company's information needs can be conceptualized to better understand them. By defining where in the cube the most critical knowledge for the company is located it can be more easily targeted, communicated and obtained. Set in the cube of business information the employees are internal sources of information, and in the context of competitive intelligence, the subject of information is external. The type of information can be both qualitative and quantitative.

Classifying information and knowledge in the context of security refers to defining who has access to it. This classification needs to be done to all information assets. Desouza and Vanapalli emphasize that private organizations could learn from the defense and intelligence organizations on how to secure critical knowledge. However, they begin from the phase when critical knowledge documents have already been tagged with a classification of top secret or classified. They pay little attention to classification or identification of knowledge that has not been documented. [30] From the viewpoint of this paper the non-documented knowledge is what is interesting. How to classify it remains still an open question.

Data or information classification frameworks such as the one introduced by Appleyard [31] can be of help when critical knowledge is assessed. It is often suggested that such classification schemes are kept simple, and following this simplicity rule Appleyard suggests a classification of important information into three classes: public, internal use only, and company confidential. [31] The rule being that the more critical to business the information is, the higher the classification class. When dealing with knowledge, the challenge is to implement this classification scheme into the minds of every employee, because there is no-one else to tag the knowledge they possess. Employee judgement needs to be influenced in order to enforce correct classification of critical knowledge.

Framework for recognizing critical knowledge

When combining the information classification schemes and the risk matrix approach to find the information assets that most need protection, the following framework can be built. When employees realize they have knowledge that they feel could be of value to the company they can assess the knowledge in the dimensions of importance and awareness. The framework is illustrated in Figure 1.

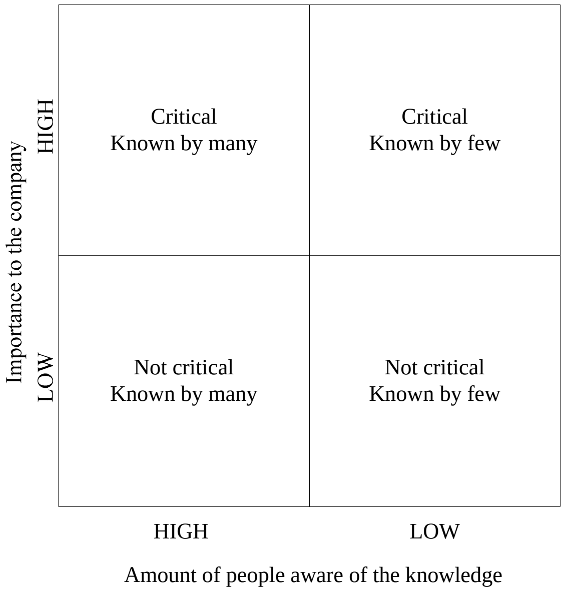

Figure 1. The framework for recognizing important knowledge

The framework is constructed from two dimensions: the importance that certain competitive knowledge has to a company and how well this knowledge is known. The more critical the knowledge and the less people aware of it, the greater the potential of the competitive advantage it may bring to a company.

The competitive knowledge in the upper right corner is the best source of competitive advantage to a company. Its implications are crucial but at the moment only few people are aware of it. This information should be shared to the decision makers that can act upon it and simultaneously it has to be protected from spreading, so that competitors will not get their hands on it.

Respectively the competitive knowledge positioned in the lower left corner is not worth to invest protective actions in. Knowledge that has got no significant affect and is widely known is not likely to be a source of competitive advantage. It is good to note that the amount of people here is in proportion to the number of employees working in the company. If 10 people have the knowledge, in a company of 1000 employees they are a few, but in a company of 20 employees they are many.

A third dimension could be added to the framework: the sources aware of information, and whether they are internal or external. If the sources are internal, i.e. employees, the competitive knowledge they possess is not as easily obtained by competitors. The value of knowledge increases when the knowledge is critical, known by few and those few are company's own employees. This also increases the need to protect that knowledge from leaking outside the company. In the context of this paper we focus on knowledge that is possessed by the employees of a company. The security perspective of this paper is not relevant to knowledge that is outside the company, although that source may be relevant from the competitive intelligence perspective.

As such this framework works mainly to spot critical bits of knowledge. The challenge in the assessment is how to decide how important a bit of information or knowledge is to the company. The framework can be used both in the company level and in the level of individual employees.

At the company level the framework can be complemented with a set of questions to help determine the importance of knowledge. The questions can be for example:

- Is the knowledge important to top management?
- Does it impact product or service development and planning?
- Does it concern customer relationships?

If the answer to such questions is yes, the importance to the company is high. The question sets need to be made company specific, as it heavily depends on the type of business what kind of knowledge is of most value.

The dimension of amount of people aware of the knowledge has meaning when considering actions on whether a piece of knowledge should be protected or not. If it is widely known inside a company, chances are that it is widely known also outside the company, and there is no need to protect. Some knowledge however might be widely known inside a company but still be of high importance.

The difficulty of positioning knowledge that is known by few in the company is the judging of importance. A rumor that a customer is planning a new way of operations might not be of high importance to a maintenance worker, but this same bit of knowledge might be critical when combined with other bits of knowledge about that customer of the industry. So the worker who hears the rumor needs to a) realize that the managers might need that bit of knowledge, b) share it with the appropriate persons, and c) not tell it to anyone else. In the employee level the framework can thus be utilized as a tool for awareness training.

How to act with critical competitive knowledge

Critical competitive knowledge can be secured in the company when it has been recognized as critical. The above described framework can be used to structure the training and awareness programs inside companies. Once employees recognize that what they know can be characterized as critical competitive knowledge they can act accordingly.

What to do with critical knowledge depends on the type of knowledge in question. If the knowledge is known by many, the key is to emphasize the meaning of that knowledge to the company so that employees are aware of its importance. The knowledge about a major customer’s products may not create competitive advantage, but it still is critical in the sense that it cannot leak outside the company, or the company will lose the customer and possibly suffer other consequences too.

When a bit of knowledge is known only by a few employees, and is of high importance to the company the awareness of who to share that knowledge with becomes essential. The training offered in the company needs to emphasize the kinds of knowledge that the executives use to make decisions, so that employees recognize it. The question sets described in the previous section can be useful in awareness training.

An ideal situation for a company would be that a company has most of its knowledge in the top right and bottom left corners of the framework. That would mean that business critical knowledge would be known only by a limited amount of people and that all other knowledge would be widely spread in the company. Since such a situation is very difficult to reach, the security and intelligence functions aim to build awareness into the company so that critical knowledge, even if widely known is kept safe. Also knowledge that is not widely known should be reasonably shared so that potentially critical knowledge is spotted and useful knowledge is put into wider use.

Conclusions and implications for further work

This paper has discussed the importance of employee awareness of critical knowledge and the perspectives of both security and intelligence to that knowledge. Knowledge security works toward securing important knowledge assets, where as competitive intelligence aims to the efficient sharing of them. At first glance these two seem opposite approaches to the same issue. However, a lot of similarity can be seen in these approaches.

Sharing knowledge or even articulating the need for a certain kind of knowledge does not have mere positive effects but poses also risks. Sometimes revealing a need can also reveal strategic information that might do the company a lot of harm if ended up in public. Sharing knowledge has risks, and some knowledge should not be shared even inside the company other than on a need-to-know basis. Employees need to be aware of executive knowledge needs so that when they come across a bit of knowledge that they feel is of importance, they know what to do. Sometimes it may be only after the decision has already been made that employees can be told what the meaning of the knowledge was, but to the benefit of future situations it should be done.

The process of securing knowledge can create risks also from the employee satisfaction perspective. If employees are not allowed to openly discuss company issues, and are not told how executives use the knowledge they are provided with, it can cause dissatisfaction. The framework introduced in this paper works as a means of communicating both the competitive knowledge and knowledge security perspectives of knowledge to employees.

Further analysis of this framework could be done by testing it in actual companies and refining the question sets complementing the framework. The perspective of competitive intelligence would also suggest the dimension of persons outside the company being added to the framework.

An interesting question to be discussed further is how companies can choose a method of efficient knowledge sharing that is both secure and adequately supports the competitive knowledge needs in the company. This brings also the perspective of knowledge management to this already interdisciplinary framework.

References

[1] Ericksson, M. “Organizing Intelligence Requires More than Key Intelligence Topics”, *Competitive Intelligence Magazine*, 1(11), January/February, 2008, pp. 16-20.

[2] Kinsinger, P. “Repositioning Competitive Intelligence: From Serving the Few to Empowering the Many”, *Competitive Intelligence Magazine*, 5(11), September/October, 2008, pp. 8-15.

[3] M. C. Drott, “Personal Knowledge, Corporate Information: The Challenges for Competitive Intelligence”, *Business Horizons*, 2(44), 2001, pp. 31–37.

[4] Fleisher, C.S. “*The Present and the Future of Business and Competitive Intelligence*.” A presentation at ComBI seminar in Tampere University of Technology, September 19th 2008. Unpublished.

[5] Fleisher, C.S., and Bensoussan, B.E. “*Business and Competitive Analysis. Effective Application of New and Classic Methods*.” Pearson Education, New York. 2007.

[6] Badr, A., Madden, E. and Wright, S. “The Impact of Competitive Intelligence on the Development and Implementation of Strategy

in the Pharmaceutical Industry”, *Journal of Competitive Intelligence and Management*, 3(4), 2006, pp. 15-35.

[7] Bose, R. “Competitive Intelligence Process and Tools for Intelligence Analysis”, *Industrial Management and Data Systems*, 108(4), 2008, pp. 510-528.

[8] Collins, R. J. *Better Business Intelligence. How to Learn More About Your Competitors*. Chalford, Management Books 2000. 1997.

[9] Cook, M. Cook, C. *Competitive Intelligence. Create an Intelligent Organization and Compete to Win*. Kogan Page Limited, London. 2000.

[10] Saayman, A. Pienaar, J. de Pelsmacker, P. Viviers, W. Cuyvers, L. Muller, M-L. and Jegers, M. “Competitive Intelligence: Construct Exploration, Validation and Equivalence”, *Aslib Proceedings: New Information Perspectives*, 60(4), 2008, pp. 383-411

[11] Thierauf, R. *Effective Business Intelligence Systems.* Westport, Quorum Books. 2001.

[12] Vitt, E. Luckevich, M. Misner, S. *Business Intelligence – Making Better Decisions Faster.* Redmond, Microsoft Press. 2002.

[13] Dutka, A. *Competitive Intelligence for the Competitive Edge*. NTC Business Books, Chicago. 1998.

[14] Fleisher, C.S. “An Introduction to the Management and Practice of Competitive Intelligence (CI)”, in: Fleisher, C.S. and Blenkhorn, D.L. (eds.) *Managing Frontiers in Competitive Intelligence*. Quorum Books, Westport. 2001.

[15] Butcher, H. *Meeting managers’ information needs.* A managing information report, Aslib, The Association for Information Management. Staple Hall, London. 1998.

[16] Frishammar, J. “Information Use in Strategic Decision Making”. *Management Decision*. 41(4), 2003, pp. 318–326

[17] Pirttilä, A. *Kilpailijaseuranta*. WSOY, Porvoo. 2000.

[18] Choo, C. W. *Information Management for the Intelligent Organization. The Art of Scanning the Environment.* 3rd Edition. Information Today, Inc., Medford. 2002.

[19] Drott, M. C. “Personal Knowledge, Corporate Information: The Challenges for Competitive Intelligence”, *Business Horizons*, 2(44), 2001, pp. 31–37.

[20] Pirttilä, A. *Competitor information and competitive knowledge management in a large, industrial organization.* Doctoral thesis, Lappeenranta University of Technology. 1997.

[21] *Collins English Dictionary* 8th Edition, HarperCollins Publishers. 2006.

[22] Bojanc, R. Jerman-Blazic, B. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28, 2008. pp. 413-422

[23] Taleb, N. N. *The black swan: the impact of the highly improbable.* Penguin Books, London. 2008.

[24] Peltier, T. Peltier, J. Blackley, J. *Information Security FUNDAMENTALS*. Auerbach publications, Boca Raton, FL. 2005.

[25] von Solms, B. von Solms, R. “The 10 deadly sins of information security management”. *Computers & Security*, 23, 2004. pp. 371-376.

[26] Desouza, K. *Managing knowledge security: strategies for protecting your company’s intellectual assets.* Kogan Page Ltd, Philadelphia. 2007.

[27] Broome, P. “Making Competitive Intelligence Work for the Small Business.” In C. S. Fleisher & D. L. Blenkhorn (Eds.), *Managing Frontiers in Competitive Intelligence: Lessons from the Trenches* (pp. 200-209). Wiley, New York. 2001.

[28] Vuori, V. “Business Intelligence Activities in Construction Companies in Finland – A Series of Case Studies”. *Proceedings of the 8th European Conference on Knowledge Management*, 2007. pp. 1086–1092.

[29] Hannula, M. & Pirttimäki, V. ”A Cube of Business Information”. J*ournal of Competitive Intelligence and Management.*. 3(1), Special SCIP04 Conference Issue Autumn 2005, pp. 33-40.

[30] Desouza, K. Vanapalli, G. “Securing knowledge in organizations: lessons from the defense and intelligence sectors”. *International Journal of Information Management*, 25(1), February 2005, pp. 85-98

[31] Appleyard, J. ”Information Classification: A Corporate Implementation Guide”. In Tipton, H. Krause, M. (eds.) *Information Security Management Handbook.* Fifth edition. USA, CRC Press. 2004.