THE RISK ASSOCIATED TO THE KNOWLEDGE TRANSFER AT ORGANIZATIONAL LEVEL

Mirela GHEORGHE[1]

ABSTRACT
The purpose of this paper is to present the concept of knowledge transfer risk, the specific features of this type of risk in inter-organizational and intra-organizational environments. The motivation for this research originated from the necessity of an analysis of the risk involved in the process of knowledge transfer, in the present context of the knowledge based society. Knowledge, knowledge management, knowledge transfer, knowledge transfer risk, knowledge transfer security are concepts associated to the actual business trend characterized by the growing globalization phenomena, global competitiveness, ever changing dynamics and high data amounts that demand real-time decisions on any manager.

KEYWORDS: *knowledge risk, knowledge transfer, knowledge security, risk, uncertainty*

JEL CLASSIFICATION: *M20, M21*

INTRODUCTION

In the last decade of the 20th century and the beginning of the 21st century, the knowledge has gained new meanings and significance relative to the classical and modern philosophies. Knowledge is no longer a human mental process, but one belonging to artificial intelligence systems, to organizations. Across the ages, the problem of knowledge has been confronted with numerous controversies, evolving from the concept of knowledge as mental state, to the modern theories that support artificial intelligence as a form of knowledge despite the lack of human conscience.

The 21st century's philosophy will take into account the importance which all the shapes of knowledge gain in the *Knowledge society*. Apart from the scientific knowledge, in day to day language we can find various forms of knowledge that answer to questions such as: *know-how, know-where, know-why, know-that, know-if*. Knowledge implies the ability to apply the information, whether consciously or not, in order to resolve a certain issue. Knowledge isn't based only on accumulating actions, but it includes the experience and the ability of executing certain judgments which can be used to coordinate those actions.

Organizations based on knowledge are clever players of the information society and have a decisive role in its assertion as a society belonging to knowledge. In the knowledge based society, the decisive processes are those largely nominated by the expression of the "3I"s, more precisely "Innovation" (the creation of new knowledge), "Learning" (acquiring new knowledge) and "partnership Interactivity" regarding knowledge. In this framework, both inter-organizational and intra-organizational knowledge transfer represent the fundamental process for generating knowledge.

The present paper offers an analysis of the risks that can occur in the process of knowledge transfer, risks which although seem to cover only the level of communication between two players (source and recipient), actually go beyond this border. The used methodology relies on activities specific to

[1] *ASE Bucharest, Romania, mirelaghe@gmail.com*

descriptive research, starting from a theoretical approach relative to the concept of risk and uncertainty; it evolves into identifying the risk factors of the transfer knowledge in inter-organizational and intra-organizational environments in order to end with elements regarding information and knowledge security.

1. RISK AND UNCERTAINTY

In the present environment, inherent for the knowledge based society, which is characterized by a high competitiveness, ever changing dynamics, uncertainties and endless changes, the activity of any organization is carried out under risk and uncertainty conditions. Incomplete or incorrect knowledge of one or more variables is a defining feature of present day economic activities. Uncertainty and risk affect estimation accuracy regarding future evolutions and results of the organization.

Any economic activity implies a certain degree of risk that can be more or less anticipated. If by uncertainty we understand exhibiting a doubt regarding the occurrence of a future event, the risk represents a notion that has an economics, social, human, political and natural dimension which reflects the possibility that a certain activity from the future will produce a loss generated by the lack of information or its insufficient value at the decision making moment. Determining the sources of some unwanted consequences generated by a certain risk can be done using probabilities, unlike deterministic theory that presumes that all activities take place under completely known conditions.

Although the terms *risk* and *uncertainty* are used often in various combinations, there is a clear difference between them. This difference is made for the first time by Frank Knight. In the vision of Knight (Knight, 1921), ***the risk*** is limited to the situations in which the decision maker can attach mathematical probabilities to random events that can occur. ***The uncertainty*** refers to situations in which the events cannot be expressed in terms of mathematical precise probabilities, fact that determines Knight to state the following: "*the risk is a measurable form of uncertainty, as opposed to an unmeasurable uncertainty*".

Otherwise said, ***uncertainty*** "*represents the fact of not knowing in advance what is going to happen in the future. The risk is the way in which we characterize how much uncertainty there exists. The more uncertainty exists, the greater the risk will be and vice-versa. The risk therefore represents a characterization of the degree of uncertainty*" (Knight, 1921).

The degree of uncertainty of a business is given by those risks that cannot be identified inside an organization at a given moment, while the degree of risk is given by the identified risks. The greater the weight of unidentified risks is in a certain situation, the more unclear is the evolution of the analyzed activities. Even if the decision maker knows most of the risks involved in his actions, it is possible that the uncertainty will not disappear totally.

Another vision regarding the difference between ***risk*** and ***uncertainty*** is associated to the notions of ***information*** and ***knowledge***. Uncertainty is always associated with the lack of information and refers to a state, characterized by doubt and which comes from the lack of knowledge about what will happen or not in the future. Uncertainty varies according to the amount of knowledge each individual holds, in tight relation with his attitude regarding risk, under the same conditions two individuals can have different attitudes. For example, it can be observed that decision making under the state of uncertainty is based more on intuition than solid information, so we can say that if the probability of an event to occur is known we can make righter reasoning under risk conditions than under uncertainty conditions.

Traditionally, many specialists have analyzed and evaluated the risk at the organization level starting from the assumption that the risk is an uncertain element, which can generate financial losses or other negative and irreversible effects. Beginning with the 21st century, risk analysis switched to a more complex approach that determines the risk to be looked at both as a threat but also as an opportunity.

2. THE RISK IN THE KNOWLEDGE TRANSFER

Knowledge transfer is considered to be the process through which knowledge is transmitted between a source and a recipient that unlike information transfer requires de- and re-contextualization of knowledge. Success of the transfer can be determined e.g., by the extent to which the source's knowledge is recreated at the recipient (Cummings & Teng 2003).
When talking about knowledge transfer we should first do some distinctions with decisive implications regarding the understanding of the phenomenon, because the transmission of knowledge differs from the transmission of information (Blebea, 2011). The transfer of knowledge implies the transfer of information, but it also assumes generating new knowledge based on intelligence and creativity.

Figure 1. The components of the knowledge transfer

Starting from this definition, we ask ourselves which could be the risks associated to the process of knowledge transfer?
Szulanski was one of the first authors that empirically studied the risk factors associated to the knowledge transfer; three major factors result from his workings (Szulanski, 1996):

- Causal ambiguity of knowledge;
- Reduced integration ability of the recipient's knowledge;
- Emitter - recipient communication relation.

In the literature, knowledge risk is defined as operational risk that is caused by a dependency on, loss of, unsuccessful intended or unintended transfer of knowledge assets and results in a lack or non-exclusivity of these assets (Bayer F. & Ronald M., 2006).
Analyzing the components of the knowledge transfer process (figure no.1), **the risk factors** could be assign to each component as it follows:

- The skill of the knowledge transmission source;
- The nature, the form and the complexity of the transmitted knowledge;
- The recipient's ability to absorb and to generate new knowledge.

Furthermore, the analysis of the risk factors can be customized depending on the context of the inter- and intra-organizational knowledge transfer.

Inter-organizational knowledge transfer is the main interest and it is initiated deliberately or not by the source, randomly, or it is initiated with a purpose by the beneficiary.
The risks associated to the knowledge transfer between organizations depend on a series of factors, among which we mention: source and recipient, knowledge and the context in which the transfer is executed.

1. **The characteristics of the source and recipient** include, for example, the ability of the source to explain the knowledge, the reliability of the source, the ability of the recipient to absorb knowledge, assimilation, knowledge transformation and utilization, and also the motivation of both partners (Szulanski, 1996). The high values of these characteristics have a positive influence on the transfer of both the wanted knowledge and the unwanted knowledge.

2. **The characteristics of the knowledge** feature, for example, ambiguity, specificity, complexity, dependency to other knowledge. Furthermore, these characteristics, applied to a knowledge transfer, explain the difficulties of the recipient from the perspective of recreating the value. This means that the risk of an unintentional knowledge transfer decreases, but the risk of an intentional knowledge transfer grows, but without success, with these characteristics.

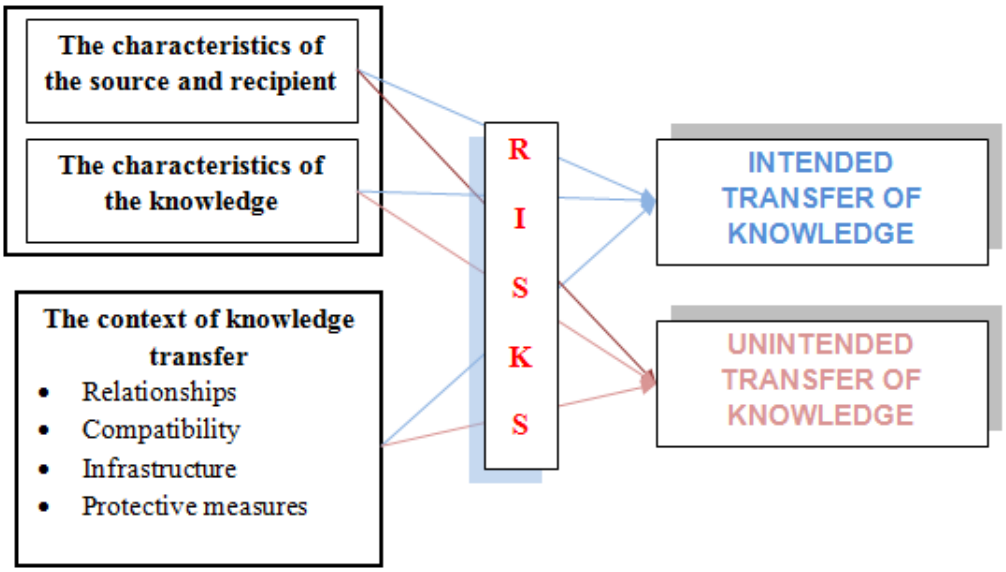

Figure 2. Risk factors in the inter-organizational knowledge transfer
(source: adapted by Bayer F.& Maier R., 2006)

3. **The characteristics of the context in which the knowledge transfer is executed** can be divided into characteristics associated to partnerships (competition versus collaboration, relations based on trust versus opportunism), compatibilities (business practices, organizational culture and knowledge level), infrastructure (internal structures, compatible IT systems), protective measures (security policies, transfer policies, intellectual property rights).

Approaching knowledge transfer risks must not inhibited collaboration and communication with business partners. Basically, blocking the transfer can prove "bilateral" meaning that it will inhibit also the wanted inflow of information from the outside towards the inside.

Risk management policies must not transform the organization into an autarchic organism, which refuses communication and collaboration with partners and the outside environment in general.

Generalized transfer control can badly influence an organization by denying it from the information influx from the outside towards the organization, influx that cannot harm, but help that organization.

In the context of **intra-organizational knowledge transfer**, the risk factors can be associated to the following elements:

1. The relationship between the two players: *source-recipient* an essential factor for a successful transfer;
2. The nature of the knowledge;
3. The way the knowledge transfer is mare;
4. The knowledge "reservoirs" from within the organizations.

Together with the motivational constraints and the elements specified previously other risk generating factors can be added such as: the lack of reward, of commitment, resistance to change, inappropriate attitude among employees or departments, difficulties encountered during the "learning" process.

Argote L., McEvily B. & Reagans R. (Argote L. & all, 2003) have proposed an analysis frame of the risks in the knowledge transfer starting from 3 dimensions: the characteristics of the entities participating at the process, the characteristics of the relationships between entities and the characteristics of the knowledge.
Markus C. Becker and Mette Praest Knudsen (Markus & Mette, 2003) complete this analysis frame and consider that knowledge transfer risk factors, established at an inter- or intra-organizational level, can be analyzed from the point of view of 6 elements:

- The characteristics of the environment (of the network) between the two included entities;
- The characteristics of the relationship between entities;
- The characteristics of individual actors (employees – attitude, motivation and abilities);
- The characteristics of each organization (organizational structure, business practices);
- The characteristics of the knowledge (ambiguity, complexity, specificity);
- The characteristics of the mechanisms of transfer knowledge.

3. KNOWLEDGE SECURITY

The security, the protection of the data, of the information and of the knowledge, which builds the value asset (intellectual capital) in a knowledge based society, is essential for the competiveness and the perenniality of an organization.
In the vision of the 27001 ISO standard (ISO_27001, 2005), ensuring information security supposes 3 fundamental objectives:

- **Confidentiality**: the objective through which it is ensured that the information is accessible only to those authorized;
- **Integrity**: the objective through which the accuracy and the completeness of the information from the system is ensured;
- **Availability**: the objective through which uninterrupted access to the information in the system is ensured for authorized users, regardless if events with destructive character have occurred (shutdown of electric energy supply, tension fluctuations, natural disasters, accidents, attacks).

By which means would the security of the knowledge differentiate from the security of the information?
The answer to this question comes from the definition of knowledge versus the definition of information. Knowledge is dynamic, fluid and much more movable than information. Knowledge includes both silent but also explicit knowing, which often cannot materialize into touchable assets. Therefore, **knowledge security** could be marked out by using three defining elements: *the security of the assets* which include knowledge, *the security of the processes*, *technologies* and *services* which engulfs knowledge and *the security of the human factor* that possesses knowledge.

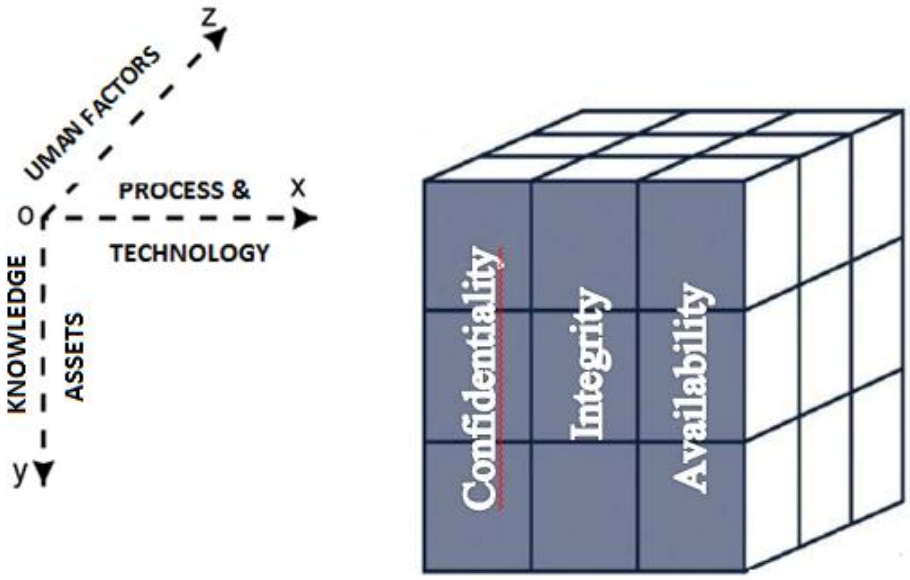

Figure 3. Knowledge security

The security of knowledge imposes in a first step identification of the threats and vulnerabilities that threaten the intellectual capital of a company. Incidents such as information leaks which affect the rights of intellectual property represent a risk often brought up in the business environment. A proactive approach of identifying the vulnerabilities over the knowledge assets of the organization, especially in collaborative working medium (multinational companies), could help design dynamic and efficient security policies.

4. CONCLUSIONS

The knowledge based society not only that cannot eliminate the traditional concept, but must accept the necessity for reconsidering and readapting it to a new dimension, the one of the knowledge transfer associated risk. The necessity of analyzing and evaluating this risk becomes the key process at the level of any entity, of which any manager must be aware and to which he must find optimum solutions so that its organization remains competitive under the circumstances of an ever more dynamic and unstable market.

The risk associated to the knowledge transfer delineates on each of its component: the actors involved (source and recipient), knowledge (through their complexity, specificity and ambiguity) and the context in which knowledge transfer occurs. Moreover, the risks can be particularized depending on the type of knowledge transfer, whether it is intra- or inter-organizational. The necessity of ensuring knowledge transfer security becomes a "sine qua non" condition in the present context. More and more researchers, specialists and practitioners state that, in recent years, knowledge represents the most important source of competitive advantages for organizations. Granting more attention to knowledge management, having in focus the enhancement the organization's performance, consists in increasing the design, attainment and implementation efforts of instruments, processes, systems, structures and cultures which will contribute to optimizing the processes of obtaining, storing, protecting and using of all the types of important knowledge for an organization's performance.

ACKNOWLEDGEMENTS

This work was co-financed from the European Social Fund through Sectorial Operational Programmer Human Resources Development 2007-2013, project number POSDRU/89/1.5/S/56287 „Postdoctoral research programs at the forefront of excellence in Information Society technologies

and developing products and innovative processes", partner Bucharest Academy of Economic Studies – Research Center for "Analysis and Regional Policies.

REFERENCES

Argote L., McEvily B., Reagans R. (2003). *Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes*.

Bayer F., Maier R. (2006). *Knowledge Risks in Inter-Organizational Knowledge Transfer*, Proceedings of I-KNOW 2006 Graz, Austria.

Blebea Nicolae Gabriela (2011), *Knowledge transfer, ongoing support*, Bucharest.

Cummings, J. L., Teng, B. S (2003). *Transferring R&D knowledge – the key factors affecting knowledge transfer success,* Journal of Engineering and Technology Management.

Knight F.H. (1921) *Risk, Uncertainty and Profit*, Houghton Mifflin Company, Boston.

ISO_27001 (2005). *Information technology - Security techniques -Information security management systems - Requirements.*

Markus C. Becker, Mette P. Knudsen (2003), *Intra and Inter-Organizational Knowledge Transfer Processes: Identifying the Missing Links,* DRUID Working Paper No. 06-32.

Sveiby K.E. (2000), *La nouvelle richesse des entreprises. Savoir tirer profit des actifs immateriels de sa societe,* Maxima, Paris.