2014

A CONCEPTUAL FORMATIVE FRAMEWORK OF KNOWLEDGE RISK GOVERNANCE TO ENHANCE KNOWLEDGE SHARING

Azadeh Sarkheyli
Universiti Teknologi Malaysia, sazadeh2@live.utm.my

Rose Alinda Alias
Universiti Teknologi Malaysia, alinda@utm.my

Norafida Binti Ithni
Universiti Teknologi Malaysia, afida@utm.my

A CONCEPTUAL FORMATIVE FRAMEWORK OF KNOWLEDGE RISK GOVERNANCE TO ENHANCE KNOWLEDGE SHARING

Azadeh Sarkheyli, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, sazadeh2@live.utm.my

Rose Alinda Alias, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, alinda@utm.my

Norafida Binti Ithnin, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia, afida@utm.my

Abstract

The issue of security has been a controversial and much disputed subject within the field of Knowledge Sharing (KS). We have previously drawn attention to the paradox in KS security and Information Systems (IS) security. Far too little attention has been paid to integrate security into KS. Thus, this study proposes a conceptual framework of Knowledge Risk Governance (KRG) to illustrate how governance of KS risks can be applied to decrease the risks of KS. To understand how KS could be improved, we draw upon Social Exchange Theory (SET) to examine and improve KS behavior. The potential constructs for the KRG framework were identified through literature review. Therefore, the main objective of this paper is to investigate factors of the KRG framework. Finally, this paper demonstrates the importance of the KRG framework to enhance KS.

Keywords: Knowledge Sharing, Knowledge Sharing Risks, Knowledge Risk Governance

1 INTRODUCTION

Knowledge could be defined as a composition of various tangible and intangible things such as experience, values, expert knowledge, contextual information which are useful for incorporating the new experience and information into actions. Knowledge is more intangible, because it exists in persons' minds and it is demonstrated through their behaviors and actions, and not only in documents and repositories (Gammelgaard & Ritter, 2000; Asllani & Luthans, 2003; Gold et al. 2001). In the new economy, Knowledge Sharing (KS) as one of the main issues of Knowledge Management (KM) is very significant for all organizations. It is a key process in creating new products and services, in leveraging organizational knowledge assets and in achieving collective outcomes. However, research on KS also revealed its complex nature and highlighted a multitude of factors that impede KS in and between organizations. KS success is defined by capturing and getting the right knowledge to the right users, and using this knowledge to enhance organizational and/or individual performance (Jennex & Zyngier, 2007).

To understand how KS could be improved, we draw upon Social Exchange Theory (SET) to examine and improve KS behavior. Thus, it will be scrutinized among three levels of SET analysis which are individual, group and organization. SET has been one of the most popular theories in explaining KS. According to SET, people share their knowledge because of their perception of the benefits that may result from such behaviours (Liang et al, 2008).

Security is a significant topic, and it is important for KS also. However, there has been little discussion on KS security. Security in KS is about transferring and sharing knowledge from knowledge producers to the users of knowledge (Sarkheyli et al., 2013). This study has reviewed the concepts of security for KS and found that there is little attention about security of knowledge sharing in the literature.

The objectives of this paper are to identify the formative variables of Knowledge Risk Governance (KRG) and to propose a formative conceptual framework of KRG. This study focuses on aspects of security that are distinctive to KS. To achieve these objectives, we will look at what KS is, risks of KS, support for decrease of KS risks through KRG framework to improve KS behavior and specify the constructs for KRG.

2 BACKGROUND OF STUDY

The growing use of knowledge in business brought to the emergence of KM (Aranda & Fernandez, 2002). Thus, KM is the assortment of processes and tools that comprehensively capture, organizes, shares, and analyzes knowledge assets which are accepted from resources, documents, and people skills within the organization. Recent evidence suggests that firms that expand and leverage resources of knowledge will be more successful than firms who are more dependent on tangible resources.

The process of KM consists of several activities. The most commonly discussed activity in the process of KM nowadays is knowledge transfer or Knowledge Sharing (KS) (Ford, 2001). KS in an organization occurs when members of an organization pass knowledge to each other (Nonaka & Takeuchi, 1995).

However to implement the security for KS we should study KM risks. Risks of KM are divided into three main categories; Risks of Knowledge Acquirement, Risks of Knowledge Sharing and Risks of Knowledge Utilization (Bing-hui, 2010). Figure 2.9 illustrate this by sub-risks in each category.

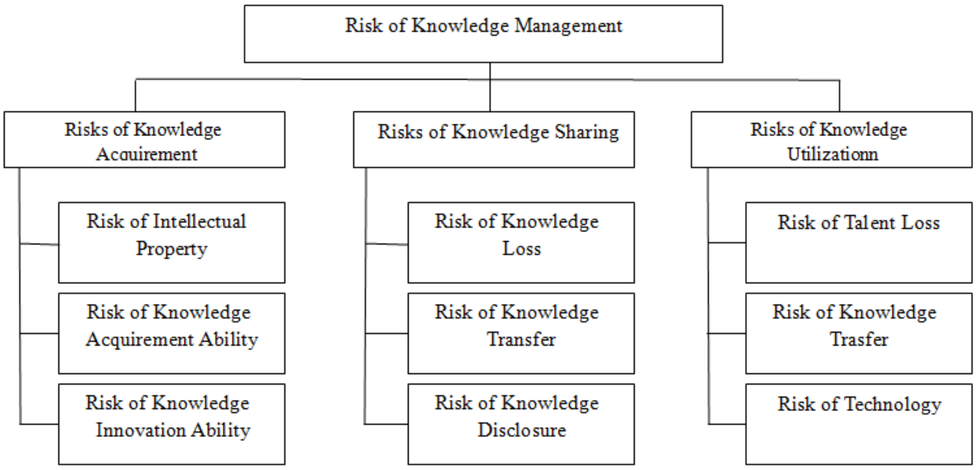
Risk of Knowledge Management
Risks of Knowledge Acquirement
Risks of Knowledge Sharing
Risks of Knowledge Utilizationn
Risk of Intellectual Property
Risk of Knowledge Acquirement Ability
Risk of Knowledge Innovation Ability
Risk of Knowledge Loss
Risk of Knowledge Transfer
Risk of Knowledge Disclosure
Risk of Talent Loss
Risk of Knowledge Trasfer
Risk of Technology

Figure 1. Different kinds of KM risks (Bing-hui.L 2010)

According the above figure 1, risks of KM is divided to three main risks, one of which is KS risks. Therefore risks of KS compared with benefits of KS will be evaluated by assessing the related risks of Knowledge Loss, Knowledge Disclosure and Knowledge Transfer.

KRG consists of knowledge sharing risks and risk governance that illustrate the application of Risk Management through governance to KS. The KRG process consists of the same steps with risk governance, but additionally requires identification of knowledge assets (Bayer & Maier, 2007).

3 RESEARCH METHODOLOGY

The research focused on three main criteria: understanding how security could be applied in KS, how senior officers in organizations govern KS for the transfer of organizational knowledge and identifying the components of KRG. Therefore, a sequential mixed method consisting of a qualitative phase to explore the conceptualization of KS risks governance, and a quantitative phase to validate the model will be adopted for this research. Literature review of findings from the previous studies on KS security are collected in order to explain variability in findings across the studies. Hence, several studies found issues affecting the governance of knowledge risks to enhance KS. The next step to validate the proposed framework, includes two case studies are provided that illustrate the relevance of KRG to enhance KS behavior.

Questionnaires will be used to collect data from case studies. After that a pilot study will be conducted to confirm the structure and content of the survey before conducting the main study. Responses are transferred from the survey to Statistical Package for Social Sciences (SPSS) and SPSS AMOS which will be used in this study. Structural Equation Modelling (SEM) is the main analysis method to test hypotheses and to identify the direct and indirect effects between the constructs of the proposed model. Furthermore, the reliability of each factor is calculated by using Cronbach Alpha. In addition, Confirmatory Factor Analysis will be used to test the validity of the model measurements. Also, the goodness-of-fit overall model will be tested. Thus, in this paper, developing an instrument for survey and testing of the research conceptual framework is useful for future research.

4 RESEARCH FRAMEWORK AND HYPOTHESIS

Identification of knowledge assets affected by knowledge risks is required for visibility of these assets is a necessary precondition for the identification of knowledge risks. Consequently, established KM initiatives or approaches concerning intellectual capital management are favorable. Identification of knowledge risks can use different sources such as review of contracts, policies and their compliance, penetration tests for IT systems or analysis of dependencies on knowledge assets. Identified knowledge risks have to be assessed concerning probability of occurrence and severity of resulting losses. This assessment has to be based on the value of knowledge assets and also the interactions between them. However, valuation of knowledge assets is still in its infancy and thus the assessment of knowledge risks is still problematic.

KRG means the set of processes and policies affecting the way the handling of knowledge is directed, administered or controlled. Evaluation of knowledge risks concludes the security measures which are divided to three main categories; Organizational, technical and Legal. Consequently, governance describes structures and processes for collective decision making involving governmental and non-governmental actors. (Neye & Donahue 2000).

For the third criterion of this paper as it is mentioned before, various variables were determined through a literature survey. Therefore studies were selected for inclusion in this research only they satisfied a specific criterion. In other words, they had to be empirical and had to report the correlation between risk management and KS behaviour. Table 1 shows the list of variables included in this study.

Authors	Variables
Ward, P. & Smith, C.L. (2002), Tipton Harold F. & Krause Micki (2004), Beliles Jr, R. P. (2008), Singh Amit (2007), Bernard R (2007)	Physical Access Policy (PAP)
Von Solms R.(1998,1999), Danchev Dancho (2003), Fulford Heather, Doherty Neil F. (2003), Weber Rolf H. (2010), Whitman Michael E. (2004), Herath T., Rao HR. (2009), Fenn C et al. (2002), Magklaras GB, Furnell SM (2001)	IT Security Policies (ITSP)
Kwasnik Barbara H. (2000), Barclay, R. O., & Murray, P. C. (1997), Perrott Bruce E. (2007), Alavi, M., & Leidner, D. E. (2001), Tserng H.P. et al. (2009)	Knowledge Classification Policy (KCP)
Hemphill, T., & Vonortas, N. (2003), Goh S & Richards G (1997), Garvin, D.(1993), Senge, P.(1990,1992)	Reduction of Dependencies (RD)
Stevens John M. & Bagby John W. (2008), Jacobson N, Butterill D & Goering P(2004), Rossi F(2010), Cowan, R., Soete, L., & Tchervonnaya, O. (2001), Wellings P(2008), Lucas L & Ogilvie DT(1999), Barbieri E. (2010)	Knowledge Transfer Policies (KTP)
Nicol, David M.et al. (2008), Hagen, W. Alexander (2001), Hoffman, L., & Clark, P. C. (1991), Aboba, B. D.et al. (2007), Molnar, D., Soppera, A., & Wagner, D. (2005), Paulauskas, N., & Garsva, E. (2006)	Network Access Policy (NAP)
Vermeylen S. et al.(2008), Brush SB, Stabinsky D(1996); A Arora (1995), Thurow L.C. (1997), Murray F, Stern S (2007), Raysman, R., & Brown, P. (2008), Lemley A. (2004); Brad, Sherman; Lionel Bently (1999), Khemani R. S. and Shapiro D. M. (1993), Zecchini S. (1993)	Intellectual Property Rights (IPR)
Dulipovici A. & Baskerville R.(2007), Fleming L. & Marx M. (2006), Moffat Viva R. (2010), Perry JS. & Herd TJ. (2004), Alvarez, S. A., & Barney, J. B. (2001), Berger & Luckmann (1967), Latour (1987)	Non-Compete Agreements (NCA)
Klee M.M. (2000), Arkko J & Bradner S (2008), Klaila, D., & Hall, L. (2000), Gayton, Cynthia M (2006,2008)	Non-Disclosure Agreements (NDA)

Table 1. Variables used in this research

This paper proposes a conceptual formative KRG framework that includes factors in three dimensions, namely, Organizational (Physical Access Policy, IT Security Policy, Knowledge Classification Policy, and Reduction of Dependencies), Technical (Network Access Policy and Knowledge Transfer Policy) and Legal (Intellectual Property Rights, Non-Compete Agreements and Non-Disclosure Agreements). Figure 2 shows our research framework and these factors and research hypotheses are explained as follows.

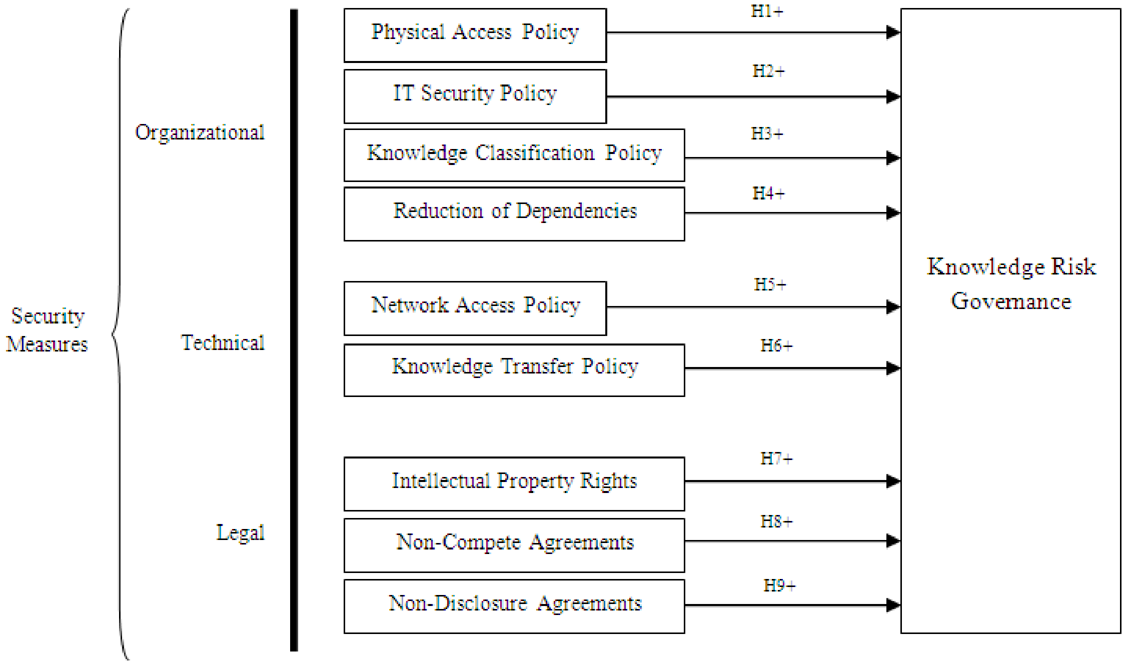
Security Measures
Organizational
Technical
Legal
Physical Access Policy
IT Security Policy
Knowledge Classification Policy
Reduction of Dependencies
Network Access Policy
Knowledge Transfer Policy
Intellectual Property Rights
Non-Compete Agreements
Non-Disclosure Agreements
H1+
H2+
H3+
H4+
H5+
H6+
H7+
H8+
H9+
Knowledge Risk Governance

Figure 2. *Conceptual framework and related hypothesis*

The assumed connection between the factors are based on an extensive literature survey, depicted in figure 2 and subsequently explained below.

4.1 Physical Access Policy

Physical Access Policy is established to ascertain the rules for the granting, controlling, and monitoring of the physical access to information/knowledge resources. Considerate what information/knowledge security means and how it affects the organisation and people is so important (Ward & Smith, 2002). By incorporating both electronic and physical information elements, previously unaddressed information security gaps can be identified and mitigated (Bernard, 2007). However, it is a security program which is related to technical support staff, security administrators, system administrators and other may have information/knowledge resource physical facility access requirements as part of their function. Thus, the physical access policy can be influenced on KRG to reduce the risks of KS. Therefore physical access policy is considered as the first major factor in the following hypothesis.

H1: Physical access policy is positively associated with KRG.

4.2 IT Security Policy

IT Security Policies are categorized in policies of IT. The area of end-user security behaviours in organizations has gained an increased attention and these safety policies are provided to different types of users of the organizations to establish requirements for each individual to follow in order to safeguard the organization and administrative information/knowledge resources (Aboba et al., 2005, Ward & Smith, 2002). These policies apply to all electronic information system resources of the organizations, including technology hardware and software owned, leased, or licensed. This includes hardware and software used to process, store, retrieve, and display and transmit electronic representations of data, voice, and video content. This leads to our second hypothesis.

H2: IT security policy is positively associated with KRG.

4.3 Knowledge Classification Policy

Knowledge could be summarized that is useful for guiding the information extraction. Knowledge classification policy enables knowledge reuse and sharing, and also gives guidance for agent adaptation. Classification schemes have properties that enable the representation of entities and relationships in structures that reflect knowledge of the domain being classified. These situation cause general knowledge to be completely reusable and can be shared for many information extraction tasks. On the other hand domain knowledge can be reused and shared for web sites in the same domain for instance (Kwasnik, 2000). Consequently, ability to reflect, discover and create new knowledge could be the benefits of this policy. Furthermore, this policy provides the opportunity to reduce the knowledge risks and we posit the following hypothesis:

H3: Knowledge Classification Policy is positively associated with KRG.

4.4 Reduction of Dependencies

In today's complex world, individuals need to help each other accomplish organizational objectives. Structures and systems in the organization need to encourage teamwork and group problem-solving by employees and reduce the dependency on upper management. Teams need to also have the ability to work cross-functionally. By working in teams, knowledge can be shared among organizational members and there is also a better understanding of other individuals, their needs and how they work in different parts of the organization, encouraging knowledge transfer as well (Senge, 1990, 1992; Garvin, 1993). Therefore, reduction of dependencies is particularly important in governance knowledge risks. Hence hypothesis 4 is posited as below.

H4: Reduction of Dependencies is positively associated with KRG.

4.5 Network Access Policy

Network Access Policy illustrates rules as a generic document for computer network access. Consequently it specifies how policies are enforced in company security or network security environment. Hence, it determines these rules for individuals or groups of individuals throughout the company. Therefore, a computer system user has some specified rights and privileges, which depend on security and Network Access Policy (Paulauskas & Garsva, 2006). Because of these Network Access Policy could be influenced on governance KS risks. This leads to the hypothesis below.

H5: Network Access Policy is positively associated with KRG

4.6 Knowledge Transfer Policy

Knowledge transfer consists of the processes and systems of support that aim to transfer knowledge, expertise and skilled people between the research environment such as higher education institutions and its user communities in industry, commerce, public and service sectors. In other words, transfer of knowledge, just like the transfer of any good, can be seen as having two main aspects; a mere physical movement and an economic circulation (Gallouj, 2000). Knowledge transfer as a policy could be suitable for governance risks of knowledge. This results in the following hypothesis.

H6: Knowledge Transfer Policy is positively associated with KRG

4.7 Intellectual Property Rights

The term "Intellectual Property Rights" refers to the legal rights granted with the aim to protect the creations of the intellect. The rights which are given to individuals over the creation of their minds could be the intellectual property rights that refer to the general term for the assignment of property rights through Industrial Property Rights (e.g. patents, industrial designs and trademarks) and Copyright (right of the author or creator) and Related Rights (rights of the performers, producers and broadcasting organizations) (Richard Raysman, et al. 2008) Based on these rights creators have an exclusive rights over the use of their creation for a specified period of time (Khemani &Shapiro,

1993). Therefore innovative thinking and decision-making are significant results of KS security through KRG. Hence Hypothesis H8 is posited below.

H7: Intellectual Property Rights are positively associated with KRG

4.8 Non-Compete Agreements

In the non-compete agreement the employee agrees to refrain from competing in exchange for a job, a promotion, or a bonus. Generally, in certain industries (e.g. information technology, telecommunication, or R&D), non-compete agreements are common. The non-compete agreements are often highly constructive to the employer and impede former employees from using the knowledge acquired during the employment. In other words, non-compete agreements regularly cite trade secrets or confidential information as the protectable interest sought to be guarded with the contract (Moffat, 2010).Therefore there is a clear need for non-compete agreements to govern the KS risks. This leads to the hypothesis below.

H8: Non-Compete Agreements are positively associated with KRG

4.9 Non-Disclosure Agreements

One of the most common ways companies and individuals protect their intellectual property is through non-disclosure agreements, hundreds of which are signed every day, throughout the world. (Klee, M.M. 2000) Non-disclosure agreements prevent the employee from using or disclosing organizational knowledge. With respect to it, none of the companies mention ‘knowledge’ and they refer to it indirectly as ‘information’. For protection of ‘information’ that corresponds in fact to tacit organizational knowledge, employees are generally asked to sign non-compete and non-disclosure agreements. Thus the hypothesis for this agreement is as follows.

H9: Non-Disclosure Agreements are positively associated with KRG

All in all, Figure 3 below illustrates a theoretical KS success framework based on the Social Exchange Theory (SET) and the proposed framework of KRG. (Therefore, the goal of this study is to develop a theoretical framework that classifies major factors into three perspectives (individual, group, and organization) to investigate whether these factors being adopted in previous studies can enhance KS behavior.) Hence, the model defines how KRG could influence improvement of KS by decreasing the KS risks.

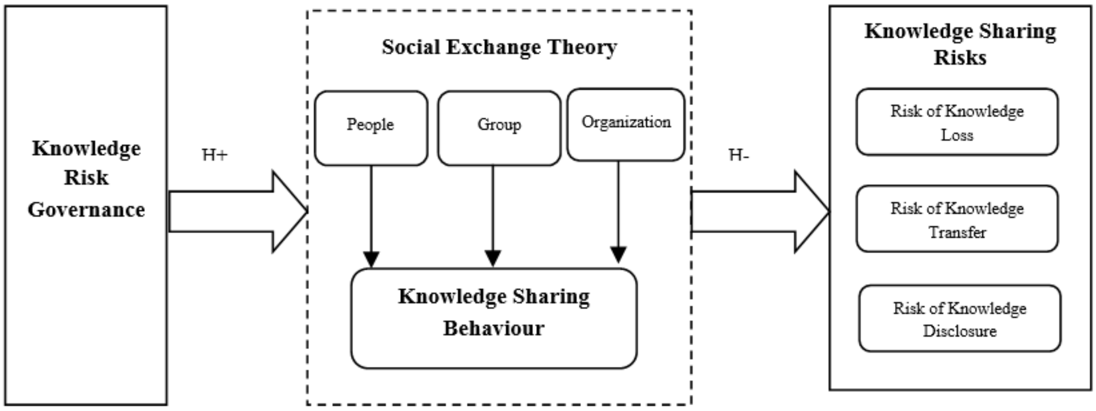
Knowledge Risk Governance
H+
Social Exchange Theory
People
Group
Organization
Knowledge Sharing Behaviour
H-
Knowledge Sharing Risks
Risk of Knowledge Loss
Risk of Knowledge Transfer
Risk of Knowledge Disclosure

Figure 3. *Theoretical framework of KS Success*

5 DISCUSSION AND CONCLUSION

This study confirms that KS is a social exchange behavior and it involves three facets of social exchange motivators which are; personal cognition, relationships among members, and organizational effort. The results of the study provide a relationship between the specific variables of security measures influencing KS behavior and KRG. The identified variables are used as the formative variables of KRG framework which is presented in this paper. These variables are recognized based on the SET which is used to explain KS behavior.

Therefore, the proposed framework of KRG is used to illustrate how security, particularly risk governance can be applied to enhance of KS. We conclude that, to have a successful strategy of KS behavior, KRG framework must be considered by senior officers.

6 FUTURE RESEARCH

The results of this research exposed a number of opportunities for managers in organizations that influence the success of implementing KS as a whole. Surprisingly, this study shows some of the security measures variables which are related to KS as formative variables of KRG. We think that research in this area especially in a public organization could have different results in a developed country. Hence, one of the important areas that we believe needs to be explored more is measurement variables of security which could be disparate in the organizations. Another significant area that needs further research is the implication of KRG on KS behavior. To provide qualitative and quantitative support for this postulation exploratory research should be conduct using case study research methodology to examine KRG within an organization context.

References

Aboba, B. D., Bensley, S. E., Eitelbach, D. L., Gidwani, N. C., Guittet, M., Palekar, A., & Paul, T. L. (2005). Method of Enforcing A Policy on A Computer Network. U.S. Patent No. 6,941,465. Washington, DC: U.S. Patent and Trademark Office.

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. MIS quarterly, 107-136.

Alvarez, S. A., & Barney, J. B. (2001). How Entrepreneurial Firms Can Benefit From Alliances With Large Partners. The Academy of Management Executive, 15(1), 139-148.

Aranda, D. and Fernandez, L. (2002). Determinants of Innovation Through A Knowledge-Based Theory Lens, Industrial Management & Data Systems, Vol. 102 No. 5, pp. 289-96.

Arora, A. (1995). Licensing Tacit Knowledge: Intellectual Property Rights and the Market for Know-How. Economics of Innovation and New Technology, 4(1), 41-60.

Arkko, J., & Bradner, S. (2008). IANA Allocation Guidelines for the Protocol Field.

Asllani, A. and Luthans, F. (2003). What Knowledge Managers Really Do: An Empirical and Comparative Analysis. Journal of Knowledge Management, Vol. 7 No. 3, pp. 53-66.

Barbieri, E. (2010). The Evaluation of Policies for Knowledge Transfer: Some Emerging Issues. International Journal of Healthcare Technology and Management, 11(4), 263-282.

Barclay, R. O. & Murray, P. C. (1997). What is Knowledge Management. Knowledge Praxis, 19.

Bayer, F. and Maier, R. (2007). Governing Knowledge Risks – Design and Results of an Empirical Study. Proceedings of I-KNOW ’07 Graz, Austria, pp 200-208.

Berger, P. L. And Thomas Luckmann 1967 The Social Construction of Reality. Garden City, NY: Anchor.

Bernard, R. (2007). Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps. Computers & Security, 26(1), 26-30.

Beliles Jr, R. P., Farino, M. W., Kolar, M. A., & Twinam, D. C. (2008). Unified Network and Physical Premises Access Control Server. U.S. Patent No. 7,437,755. Washington, DC: U.S. Patent and Trademark Office.

Bing Hui Liui and Xiao Qing LI (2010). Comprehensive Evaluation Model and Application of Risks of Knowledge Management in Supply Chain Node Enterprises. 978-1-4244-6484-5 IEEE 2010.

Brad Sherman and Lionel Bently, 1999. The Making of Modern Intellectual Property Law. Cambridge: Cambridge University Press.

Brush, S. B., & Stabinsky, D. (Eds.). (1996). Valuing Local Knowledge: Indigenous People and Intellectual Property Rights. Island Press.

Cowan, R., Soete, L., & Tchervonnaya, O. (2001). Knowledge Transfer and the Services Sector in the Context of the New Economy. MERIT, Maastricht Economic Research Institute on Innovation and Technology.

Danchev, D. (2003). Building and Implementing a Successful Information Security Policy. Online at www. windowsecurity. com.

Dulipovici, A., & Baskerville, R. (2007). Conflicts Between Privacy and Property: The Discourse in Personal and Organizational Knowledge. The Journal of Strategic Information Systems, 16(2), 187-213.

Fenn, C., Shooter, R., & Allan, K. (2002). IT Security Outsourcing: How Safe Is Your IT Security?. Computer Law & Security Review, 18(2), 109-111.

Fleming, L., & Marx, M. (2006). Managing Creativity in Small Worlds. California Management Review, 48(4).

Ford, D. (2001).Trust and Knowledge Management: The Seeds of Success. Queen's KBE Center for Knowledge-Based Enterprises, Queen's University, Kingston, ON, Canada, available at: http://business. queensu.ca/knowledge/workingpapers/working/working_01-08.pdf (accessed 26 August 2004).

Fulford, H., & Doherty, N. F. (2003). The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. Information Management & Computer Security, 11(3), 106-114.

Gallouj, F. (2000). Knowledge-intensive Business Services: Processing Knowledge and Producing Innovation/ Proceedings of the International Conference "The Economics and Socio-Economics of Services: International Perspectives" (Lille-Roubaix, 22 and 23 June 2000),vol.2: 57 - 76.

Gammelgaard, J. and Ritter, T. (2000). Knowledge Retrieval Process in Multinational Consulting Firms. Danish Social Sciences Research Council, Frederiksberg, Denmark, available at: http://web.cbs.dk/ departments/int/seminarpapers/JG-Knowledge.pdf (accessed 4 September 2004).

Garvin, D.A. (1993). Building a Learning Organization. Harvard Business Review, July- August 1993, pp. 78-91.

Gayton, C. M. (2006). Legal Issues for the Knowledge Economy in the Twenty-first Century. Vine, 36(1), 17-26.

Goh, S., & Richards, G. (1997). Benchmarking the Learning Capability of Organizations. European Management Journal, 15(5), 575-583.

Gold, A.H., Malhotra, A. and Segars, A.H. (2001). Knowledge Management: An Organizational Capabilities Perspective. Journal of Management Information Systems, Vol. 18 No. 1, pp. 185-214.

Hagen, W. (2001).Integrating Public and Private Network Resources for Optimized Broadband Wireless Access and Method.

Hemphill, T., & Vonortas, N. (2003). Strategic Research Partnerships: A Managerial Perspective. Technology Analysis & Strategic Management, 15(2), 255-271.

Herath, T., & Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, 47(2), 154-165.

Hoffman, L., & Clark, P. C. (1991). Imminent Policy Considerations in the Design and Management of National and International Computer Networks. Communications Magazine, IEEE, 29(2), 68-74.

Jacobson, N., Butterill, D., & Goering, P. (2004). Organizational Factors That Influence University-Based Researchers' Engagement In Knowledge Transfer Activities. Science Communication, 25(3), 246-259.

Jennex, M. E., & Zyngier, S. (2007). Security as a Contributor to Knowledge Management Success. Information Systems Frontiers, 9(5), 493-504.

Khemani R.S. and Shapiro D.M. (1993), "An Empirical Analysis of Canadian Merger Policy", Journal of Industrial Economics, 41(2), 161-177.

Klaila, D., & Hall, L. (2000). Using Intellectual Assets as a Success Strategy. Journal of Intellectual Capital, 1(1), 47-53.

Klee Maurice M. (2000). The Importance of Having a Non-disclosure Agreement. IEEE Engineering in Medicine and Biology.

Kwasnik, B. H. (2000). The Role of Classification in Knowledge Representation and Discovery. Library Trends, 48(1), 22-47.

Latour, B. (1987). Science in Action: How to Follow Scientists and Engineers Through Society. Harvard University Press.

Lemley, M. A. (2004). Property, Intellectual Property, and Free Riding. Tex L. Rev., 83, 1031.

Liang, Ting-Peng, Liu, Chin-Chung and Wu, Chia-Itsien. "*Can Social Exchange Theory Explain Individual Knowledge-Sharing Behaviour? A Meta-Analysis*" (2008), ICIS 2008 Proceedings.

Lucas, L. M., & Ogilvie, D. T. (1999). Inter-unit knowledge Transfer in Multinational Corporations. in Third International Conference on Organizational Learning, Lancaster, UK.

Magklaras, G. B., & Furnell, S. M. (2001). Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse. Computers & Security, 21(1), 62-73.

Moffat, V. R. (2010). The Wrong Tool for the Job: The IP Problem with Non-Competition Agreements.

Molnar, D., Soppera, A., & Wagner, D. (2005). Privacy for RFID Through Trusted Computing. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (pp. 31-34). ACM.

Murray, F., & Stern, S. (2007). Do Formal Intellectual Property Rights Hinder the Free Flow of Scientific Knowledge? : An Empirical Test of the Anti-commons Hypothesis. Journal of Economic Behavior & Organization, 63(4), 648-687.

Neye, J. S., and Donahue, J. (Eds.). (2000). Governance in a Globalizing World. Washington, DC, USA: Brookings Institution.

Nicol, D. M., Sanders, W. H., Singh, S., & Seri, M. (2008). Usable Global Network Access Policy for Process Control Systems. In IEEE Security & Privacy.

Nonaka, I. and Takeuchi, H. (1995).The Knowledge Creating Company: How the Japanese Companies Create the Dynamics of Innovation. Oxford University Press, New York, NY.

Paulauskas, N., & Garsva, E. (2006). Computer System Attack Classification. Electronics and Electrical Engineering, 2(66), 84-87.

Perrott, B. E. (2007). A Strategic Risk Approach to Knowledge Management. Business Horizons, 50(6), 523-533.

Perry, J. S., & Herd, T. J. (2004). Reducing M &A Risk Through Improved Due Diligence. Strategy & Leadership, 32(2), 12-19.

Raysman, R., & Brown, P. (2008). Technology Initiatives in the New Administration. Media L. & Pol'y, 18, 95.

Richard Raysman, Edward A. Pisacreta and Kenneth A. Adler. (2008). Intellectual Property Licensing: Forms and Analysis, Law Journal Press.

Rossi, F. (2010). The Governance of University-industry Knowledge Transfer. European Journal of Innovation Management, 13(2), 155-171.

Sarkheyli, A., Alias, RA, Ithnin, N, Esfahani, MD (2013) "*Dimensions of Knowledge Sharing Quality: An Empirical Investigation*", Journal of Research and Innovation in Information Systems, UTMSpace.

Senge, P. (1990). The Fifth Discipline: The Art and Practice of the Learning Organization. New York: Doubleday.

Senga, P.(1992), The Fifth Discipline, Random House, Sydney.

Singh, A., Gopal, P. M., Bangalore, M. S., & Krishnan, R. S. (2013). Physical Security Triggered Dynamic Network Authentication and Authorization. U.S. Patent No. 8,549,584. Washington, DC: U.S. Patent and Trademark Office.

Stevens, J. M., & Bagby, J. W. (2001). Knowledge Transfer from Universities to Business: Returns for All Stakeholders. Organization, 8(2), 259-268.

Syed-Ikhsan, S. and Rowland, F. (2004).Knowledge Management in Public Organizations: A Study on the Relationship Between Organizational Elements and the Performance of Knowledge Transfer. Journal of Knowledge Management, Vol. 8 No. 2, pp. 95-111.

Thurow, L. C. (1997). Needed: a New System of Intellectual Property Rights. Harvard Business Review, 75, 94-107.

Tipton, H. F., & Krause, M. (2004). Information Security Management Handbook. CRC Press.

Tserng, H. P., Yin, S. Y., Dzeng, R. J., Wou, B., Tsai, M. D., & Chen, W. Y. (2009). A Study of Ontology-Based Risk Management Framework Of Construction Projects Through Project Life Cycle. Automation in Construction, 18(7), 994-1008.

Ward, P., & Smith, C. L. (2002). The Development of Access Control Policies for Information Technology Systems. Computers & Security, 21(4), 356-371.

Weber, R. H. (2010). Internet of Things–New Security and Privacy Challenges. Computer Law & Security Review, 26(1), 23-30.

Wellings, P. (2008). Intellectual Property and Research Benefits. Lancaster University.

Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. International Journal of Information Management, 24(1), 43-57.

Vermeylen, S., Martin, G., & Clift, R. (2008). Intellectual Property Rights Systems and the Assemblage of Local Knowledge Systems. International Journal of Cultural Property, 15(02), 201-221.

Von Solms, R. (1998). Information Security Management (2): Guidelines to the Management of Information Technology Security (GMITS). Information Management & Computer Security, 6(5), 221-223.

Von Solms, R. (1999). Information Security Management: Why Standards Are Important. Information Management & Computer Security, 7(1), 50-58.

Zecchini ,S. ,Centre for Co-operation with the European Economies in Transition, & Organisation for Economic Co-operation and Development. (1993). Glossary of industrial Organisation Economics and Competition Law. Organisation for Economic Co-operation and Development; Washington, DC: OECD Publications and Information Centre.