Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 11-10-2016

Knowledge Protection for Digital Innovations: Integrating Six Perspectives

Stefan Thalmann
Know-Center & Technical University of Graz, sthalmann@know-center.at

Ilona Ilvonen
Tampere University of Technology, ilona.ilvonen@tut.fi

Markus Manhart
University of Innsbruck, markus.manhart@uibk.ac.at

Christian Sillaber
University of Innsbruck, christian.sillaber@uibk.ac.at

Knowledge Protection for Digital Innovations: Integrating Six Perspectives

Research-in-Progress Paper

Stefan Thalmann
Know-Center & Technical University of Graz, Austria {sthalmann@know-center.at}

Ilona Ilvonen
Novi Research Center, Tampere University of Technology, Finland {ilona.ilvonen@tut.fi}

Markus Manhart
University of Innsbruck, School of Management, Austria {markus.manhart@uibk.ac.at}

Christian Sillaber
University of Innsbruck, Institute of Computer Science, Austria {christian.sillaber@uibk.ac.at}

Abstract

New ways of combining digital and physical innovations, as well as intensified inter-organizational collaborations, create new challenges to the protection of organizational knowledge. Existing research on knowledge protection is at an early stage and scattered among various research domains. This research-in-progress paper presents a plan for a structured literature review on knowledge protection, integrating the perspectives of the six base domains of knowledge, strategic, risk, intellectual property rights, innovation, and information technology security management. We define knowledge protection as a set of capabilities comprising and enforcing technical, organizational, and legal mechanisms to protect tacit and explicit knowledge necessary to generate or adopt innovations.

Introduction

In our connected knowledge society, organizations benefit from exchanging knowledge with external parties but have to protect themselves against those that seek to appropriate critical knowledge (Jarvenpaa and Majchrzak 2016). Increased connectivity and current technological trends have shortened digital innovation cycles compared to traditional innovations, which makes innovations more difficult to protect. Digital innovations predominantly rely on innovative ideas and knowledge (Yoo et al. 2012). Due to the tacit nature of knowledge and its boundedness to humans, pure technical approaches cannot provide the needed level of protection

(Manhart et al. 2015; Olander et al. 2014). Rather, an integrated perspective that builds on several research fields is needed.

The protection of knowledge has so far been considered from different domains (Ahmad et al. 2014; Manhart and Thalmann 2015; Norman 2002): information technology security management, knowledge management, strategic management, risk management and innovation management. These domains tackle the Knowledge Protection (KP) issue from different angles and perspectives. However, the foci of these domains vary considerably. We argue that a comprehensive perspective on KP is needed for the following reasons: (1) Digital innovations become more intangible over time (Amara et al. 2008; Yoo et al. 2012). Knowledge-intensive innovations require different measures for protection (Ahmad et al. 2014). (2) Shorter innovation cycles of digital innovations increase the pressure to collaborate (Schilling 2015). (3) Organizations have to assimilate external knowledge from more dispersed sources on multiple sectors, locations, and cultural settings (Malecki 2010), forcing organizations to collaborate in innovation processes and to produce more complex outputs. (4) The use of social software for collaboration and knowledge management, called social knowledge environments (Pawlowski et al. 2014), creates many opportunities for knowledge sharing and can facilitate innovation processes (Kane et al. 2014). However, the use of social software impose new knowledge risks (Väyrynen et al. 2013). (5) Current trends in society, as well as the popularity of social software, increasingly blur the borders between private and business lives (König et al. 2014). This situation facilitates creativity for innovation processes but also creates additional risks of unwanted knowledge spillovers (Ahmad et al. 2014; Huang et al. 2015).

The overall research question is:

What is Knowledge Protection and what are its implications for the management of digital innovations?

Background

In knowledge management, KP is designated as a core strategy (Bloodgood and Salisbury 2001) but has received little attention to date (Manhart and Thalmann 2015). Strategic management literature mainly focuses on knowledge as an organizational asset in dyadic relationships, such as joint ventures or cooperation of large international enterprises, but neglects complex relationships, such as in networks (Hernandez et al. 2015; Pahnke et al. 2015). Risk management studies concentrate on business risks to already established organizational assets yet disregard the threats to emerging innovations (Ilvonen et al. 2015). However, first approaches to assess knowledge risks can be found, i.e. (Thalmann et al. 2014). Studies on IT security management emphasize well-categorized and classified resources and communication channels but underestimate the protection needs of knowledge that is bound to humans and communications supported by social media (Ahmad et al. 2014; Väyrynen et al. 2013). Finally, innovation management research highlights the formal protection of innovation processes by using contractual agreements in large companies (Amara et al. 2008) but rarely focuses on informal measures (Olander et al. 2014). Legal measures to ensure appropriation of IPRs are also well researched; however, measures for small- and medium-sized enterprises, such as patents, are often unaffordable (de Faria and Sofka 2010).

All of the reviewed base domains distinguish between tacit and explicit knowledge. Tacit knowledge is embodied in employees and is especially emphasized in knowledge, strategic and innovation management studies, and to some extent, in risk management research. The risk management, IPR and information security literature focuses on explicit knowledge that can be

stored in Information Systems. In addition to the tacit and explicit dimensions, the distinction between strategically important knowledge and operationally important knowledge is made. Therefore, strategic, innovation and IPR management studies emphasize strategically important, competitive knowledge, whereas the other domains highlight both strategically and operationally important knowledge or do not make this distinction.

Taking the six base domains into account, four major goals are relevant to KP, as follows: (1) protecting against unwanted leakage of knowledge, (2) assuring availability of knowledge, (3) countering unconditional knowledge sharing, and (4) appropriating revenue streams. Thus, KP aims to ensure operational and competitive advantage, and threats to knowledge are regarded as coming from both inside and outside the organization. Nondisclosure agreements for teams, awareness training programs, or interpersonal trust building are measures that stakeholders strive to implement at the individual level. Almost all the base domains focus on protection at the organizational level. The KP frameworks, security policies, and organizational measures are aimed for organization-wide implementation. At the inter-organizational level, behavioral control and trust building are used to reduce opportunistic behavior.

Research Plan

We plan a structured literature review, which will be conducted by following Webster and Watson (2002) and Schultze (2015). The review will be undertaken in three stages, as follows: (1) identifying the relevant literature, (2) structuring the review, and (3) contributing to theory.

In stage (1), we will conduct a full review of the top journals in the general IS and management fields and the top journals in the six base domains identified in the initial review (see Table 1). We will cover the issues over the last ten years since we expect the lion's share of publications on KP and digital innovations from 2005 until the present time. The selection of journals will be

based on their rankings if available (Azar and Brock 2008; Crossan and Apaydin 2010; Serenko and Bontis 2013). We will complement the review with backward and forward searches of highly cited articles (Webster and Watson 2002). To identify potentially relevant papers, we will apply the building-blocks approach (Rowley and Slack 2004), transforming relevant concepts into search statements and extending the statements by using synonyms and related terms.

In stage (2), we will supplement the search for papers with the development of a concept matrix (Webster and Watson 2002) that identifies the main elements of analysis. We will adapt the starting elements of the concept matrix from the work of Seidel et al. (2010)), such as "domain," "research methods," or "role of IS."

Table 1. Targeted journals

IS Senior Scholars' Basket of Journals: European Journal of Information Management, Information Systems Journal, Information Systems Research, Journal of AIS, Journal of Information Technology, Journal of MIS, Journal of Strategic Information Systems, MIS Quarterly General Management Journals: Management Science, Organization Science, Administrative Science Quarterly, Academy of Management Journal, Academy of Management Review					
Knowledge Management	Strategic Management	Risk Management	IPR Management	Innovation Mgmt.	Security Management
Journal of Knowledge Management International Journal of Knowledge Management Knowledge Management Research & Practice Journal of Information & Knowledge Management	Strategic Management Journal Journal of Economics &Management Strategy Long Range Planning Strategic Organization Strategic Entrepreneurship Journal	International Journal of Risk Assessment and Management Journal of Risk Research Journal of Risk Risk Management	European Journal of Intellectual Property Review Journal of Intellectual Property Rights International Review of Intellectual Property and Competition Law	Research Policy Journal of Product Innovation Management Regional Studies Technovation	Computers and Security Information and Computer Security ACM Transactions on Information and System Security IEEE Transactions on Information Forensics and Security

In stage (3), we plan to adopt the informed-inductive coding approach described by Patton (2005)), using the coding software ATLAS TI. The first goal is to develop a KP definition that incorporates the specifics of the identified base domains. Therefore, we strive to identify patterns within and across the base domains, using the concept matrix. Second, we aim to support our propositions with more comprehensive reasoning, resulting from a more profound description of the KP concept in the base domains and a more in-depth definition of the term.

Summary

In this paper, we indicated that KP has received different degrees of attention from various research domains, whose foci also vary considerably. Thus, we propose to integrate these perspectives on KP to extend the scope of IS research on digital innovations. Based on our initial literature review, we define KP as a set of capabilities comprising and enforcing technical, organizational, and legal mechanisms to protect tacit and explicit knowledge that are of strategic or operational importance to an organization. Therefore, KP focuses on both (1) external threats of leakage and exploitation by unauthorized parties and (2) internal threats of unavailability and loss. Finally, we have presented our plan on how to continue the literature review.

Acknowledgements

The Know-Center is funded within the Austrian COMET Program - Competence Centers for Excellent Technologies - under the auspices of the Austrian Federal Ministry of Transport, Innovation and Technology, the Austrian Federal Ministry of Economy, Family and Youth and by the State of Styria. COMET is managed by the Austrian Research Promotion Agency FFG.

This work has been partially sponsored by the FFG Project 855383 SALSA (ICT of the Future).

This work has been partly funded by the Finnish Foundation for Economic Education

References

Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective.," *Computers & Security* (42:May).

Amara, N., Landry, R., and Traoré, N. 2008. "Managing the Protection of Innovations in Knowledge-Intensive Business Services.," *Research Policy* (37:9), pp. 1530-1547.

Azar, O. H., and Brock, D. M. 2008. "A Citation- Based Ranking of Strategic Management Journals," *Journal of Economics & Management Strategy* (17:3), pp. 781-802.

Bloodgood, J. M., and Salisbury, D. 2001. "Understanding the Influence of Organizational Change Strategies on Information Technology and Knowledge Management Strategies." *Decision Support Systems* (31:1), pp. 55-69.

Crossan, M. M., and Apaydin, M. 2010. "A Multi- Dimensional Framework of Organizational Innovation: A Systematic Review of the Literature," *Journal of management studies* (47:6), pp. 1154-1191.

de Faria, P., and Sofka, W. 2010. "Knowledge Protection Strategies of Multinational Firms-a Cross-Country Comparison.," *Research Policy* (39:7), pp. 956-968.

Hernandez, E., Sanders, W. G., and Tuschke, A. 2015. "Network Defense: Pruning, Grafting, and Closing to Prevent Leakage of Strategic Knowledge to Rivals," *Academy of Management Journal* (58:7), pp. 1233-1260.

Jarvenpaa, S., and Majchrzak, A. 2016. "Interactive Self-Regulatory Theory for Sharing and Protecting in Inter-Organizational Collaborations," *Academy of Management Review* (41:1), pp. 9-27.

Malecki, E. J. 2010. "Global Knowledge and Creativity: New Challenges for Firms and Regions," *Regional studies* (44:8), pp. 1033-1052.

Manhart, M., and Thalmann, S. 2015. "Protecting Organizational Knowledge: A Structured Literature Review," *Journal of Knowledge Management* (19:2), pp. 190 - 211.

Manhart, M., Thalmann, S., and Maier, R. 2015. "The Ends of Knowledge Sharing in Networks: Using Information Technology to Start Knowledge Protection," *23rd European Conference on Information Systems (ECIS)*, Münster, Germany.

Norman, P. M. 2002. "Protecting Knowledge in Strategic Alliances: Resource and Relational Characteristics.," *The Journal of High Technology Management Research* (13:2), pp. 177-202.

Olander, H., Vanhala, M., and Hurmelinna-Laukkanen, P. 2014. "Reasons for Choosing Mechanisms to Protect Knowledge and Innovations," *Management Decision* (52:2), pp. 207-229.

Pahnke, E., McDonald, R., Wang, D., and Hallen, B. 2015. "Exposed: Venture Capital, Competitor Ties, and Entrepreneurial Innovation," *Academy of Management Journal* (58:5), pp. 1334-1360.

Patton, M. Q. 2005. *Qualitative Research*. Wiley Online Library.

Pawlowski, J. M., Bick, M., Peinl, R., Thalmann, S., Maier, R., Hetmank, L., Kruse, P., Martensen, M., and Pirkkalainen, H. 2014. "Social Knowledge Environments" *Business & Information Systems Engineering* (6:2).

Rowley, J., and Slack, F. 2004. "Conducting a Literature Review," *Management Research News* (27:6), pp. 31-39.

Seidel, S., Müller-Wienbergen, F., and Becker, J. 2010. "The Concept of Creativity in the Information Systems Discipline: Past, Present, and Prospects," *Communications of the Association for Information Systems* (27:1), pp. 217-242.

Serenko, A., and Bontis, N. 2013. "Global Ranking of Knowledge Management and Intellectual Capital Academic Journals: 2013 Update," *Journal of Knowledge Management* (17:2), pp. 307-326.

Thalmann, S., Manhart, M., Ceravolo, P., and Azzini, A. 2014. "An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection.," *International Journal of Knowledge Management* (10:2), pp. 28-42.

Väyrynen, K., Hekkala, R., and Liias, T. 2013. "Knowledge Protection Challenges of Social Media Encountered by Organizations," *Journal of Organizational Computing and Electronic Commerce* (23:1), pp. 34-55.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *Management Information Systems Quarterly* (26:2).

Yoo, Y., Boland Jr, R. J., Lyytinen, K., and Majchrzak, A. 2012. "Organizing for Innovation in the Digitized World," *Organization Science* (23:5), pp. 1398-1408.