3-4-2015

A Capability Model for Knowledge Protection

Markus Manhart

A Capability Model for Knowledge Protection

Markus Manhart[1]

[1] University of Innsbruck, Department of Information Systems, Production and Logistics Management, Universitätsstraße 15, 6020 Innsbruck, Austria
markus.manhart@uibk.ac.at

Abstract. Literature on knowledge protection strongly focuses on the application of measures, widely neglecting the abilities of individual firms. A capability view on firms could help to answer the question of how well they can utilize different measures for protecting knowledge. Drawing on the resource-based view, this paper proposes the concept of protection capabilities and discusses how they could help firms to protect knowledge. Protection capabilities are conceptualized as a capability model that mirrors the identification, assimilation, and application capabilities as defined in the model of absorptive capacity. As a result, firms need to develop three types of capabilities: (1) concealment to protect their resources, (2) ambiguity to protect their capabilities and (3) enforcement to protect their business strategies. This paper discusses how each capability type reduces the risk of external organizations absorbing knowledge, and gives examples of what role IT plays in building each of the capability types.

Keywords: knowledge protection, capabilities, resource-based view, absorptive capacity, knowledge-based view

1 Introduction

Literature on knowledge protection strongly focuses on the application of formal and informal measures [1-3] mainly addressing the question of *how effective can different protection measures be applied*. Characteristics like firm size [4, 5], affiliation to specific industry sectors [4, 5], or resource characteristics [6] have been identified as factors influencing the effectiveness of protection. Rarely attention has been paid to individual firms' abilities to protect. However, the effectiveness of knowledge protection depends on the individual company and situational aspects [7] and, hence, knowledge protection should be more than applying formal measures in a generalized way [8, 9]. Instead of solely focusing on how effective different measures can be applied, literature should stronger focus on *how well can a specific firm utilize different measures*. One perspective that accounts for individual organizational abilities to protect is the concept of capabilities. Capabilities are routines and processes which make use of a specific combination of resources [10, 11]. In knowledge protection literature, this capability perspective has been discussed from the resource-based view (RBV) in two ways: (1) knowledge protection as a set of capabilities itself and (2)

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Manhart, M. (2015): A Capability Model for Knowledge Protection, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 572-584

measures to reduce the risk that external organizations[1] absorb knowledge [12], or influencing factors thereof [6]. In (1), authors discuss capabilities for knowledge protection [3, 13, 14], however, do not always make clear distinctions between the concepts of capabilities and resources and, hence, it remains unclear what the nature of protection capabilities is. For (2), the focus is on proposing protection measures or identifying influencing factors of reducing the risks that externals absorb knowledge. However, this view does not focus on protection capabilities.

This paper tries to address these issues following the call by Desouza and Vanapalli [14] for a stronger focus on protection capabilities in knowledge protection literature, e.g. by developing capability models. Protection capabilities are introduced and conceptualized as a model that helps firms to reduce the risk that externals identify, assimilate, and apply knowledge as defined in the model of absorptive capacity. Moreover, the model tries to explain two things: (1) *what is protected* by the proposed capabilities, i.e. core knowledge (resource level), knowledge capabilities (capability level), or the business strategy of a firm (strategy level). And (2) *where is the impact*, i.e. on reducing the risk that externals identify, assimilate, or apply knowledge.

2 Foundations

The following foundation section is based on a profound literature review [15] and describes one specific part of it, i.e. knowledge protection from the perspective of the RBV.

2.1 Knowledge Protection

Knowledge protection is about the prevention of (a) unwanted knowledge spillovers [16], (b) knowledge loss [17], and (c) the reduction of knowledge visibility [18]. (a) Focuses on leakage of knowledge to not authorized people, (b) on leaving or retiring employees, and (c) is concerned with observability of knowledge by externals. Hence, knowledge protection focuses on the confidentiality aspect of knowledge and has to be differentiated from the wider concept of knowledge security. The latter is concerned with both external and internal confidentiality, integrity, and availability of knowledge [19] which is not the focus of this paper.

Literature on knowledge protection argues from three theoretical lenses [9]: transaction cost theory (TCE) [3], the relational perspective [6, 20], and the RBV [12, 13]. TCE scholars suggest that firms should rather use equity- based partnerships to protect knowledge. The relational perspective focuses on how relational capital, i.e. mutual trust, respect, and friendship in inter-organizational relationships helps to protect knowledge.

[1] In the following referred to as externals and described both organizations in a partnership with the focal firm as well as competitors.

2.2 Knowledge Protection and the Resource-Based View of the Firm

Scholars occupying the RBV argue that a firm can sustain its competitive advantages only when their competitors cannot acquire or imitate the firm's capabilities and resources [21], whilst there is a need to leverage resources from outside of the firm due to limited internal resources [22]. Central to RBV are the concepts of resource, capability, and business strategy. A firm's resources are input into a firm's production process [10], are manifold and can be separated into tangible resources and intangible resources [23]. Tangible ones are financial or physical resources, whilst intangible ones can be further separated into person-independent resources (intangible assets, organizational culture, routines) and person dependent resources (tacit and explicit knowledge) [23]. Capabilities are "integrated combinations, consolidations or applications of resources in an organizational context" [23]. They involve complex patterns of various resources and people, and are made up of a sequence of coordinated actions, i.e. organizational routines [10]. Substantive capabilities are routines that make use of the resources in a sense that they provide a set of decision options for a firm [11, 24]. Dynamic capabilities refer to the ability to change or reconfigure substantive capabilities [11]. After building capabilities firms have to appraise the rent-generating potential of resources and capabilities as well as to select a business strategy exploiting the resources and capabilities best, relative to external opportunities to build and sustain competitive advantage [23].

From the perspective of the RBV, there are several important implications for knowledge protection. First, during the last twelve years, knowledge-based resources became more and more recognized as critical for a firm's competitive advantage [6, 22, 23]. Hence, the protection of knowledge and knowledge capabilities becomes vital for firms to stay competitive. Second, only few scholars began to recognize the importance of capabilities to protect knowledge [e.g.,13] as they allow to incorporate peculiarities of individual firms. Third, only few scholars highlighted that effective protection of a focal firm's knowledge also depends on how it can deal with the capabilities of externals to absorb core knowledge [e.g.,12]. These capabilities of externals have been widely referred to as absorptive capacity (ACAP) and are introduced in the following.

2.3 Absorptive Capacity

Although there is a broad range of conceptualizations for ACAP [25], it is widely known as a firms' set of capabilities to identify, assimilate, and apply external knowledge to commercial ends [26]. A firm's ACAP is positively influenced by IT capabilities and complementary organizational capabilities [11]. IT capabilities are outside-in, inside-out and spanning capabilities. Outside-in refers to the identification of external knowledge, e.g. inter-organizational electronic interfaces. Inside-out refers to the application of knowledge, e.g. employees' basic IT skills. Spanning capabilities facilitate the assimilation of knowledge, i.e. the integration of outside-in and inside-out by linking new knowledge with what the firm already knows [11, 27]. Complementary organizational capabilities refer to coordination and socialization. Coordina-

tion “enhance[s] knowledge exchange across intra- and inter-organizational boundaries” [11], e.g. a team that monitors a virtual community (outside-in capability). Socialization “creates the conditions necessary to exchange knowledge” [11], e.g. shared language or common goals.

To propose capabilities that reduce the risk that externals identify, assimilate, and apply knowledge and knowledge capabilities, this paper uses ACAP as a reference model. That is because there is vast literature on ACAP [28] as a widely accepted model for explaining an organization’s ability to identify, assimilate, and utilize knowledge.

3 Towards a Capability Model for Knowledge Protection

After introducing the basic concepts, it is necessary to relate them. Therefore, it is necessary to clearly describe the concept of protective capability.

3.1 Protection Capabilities

In literature on knowledge protection the concept of capabilities has either been used synonymous to that of resource or the differentiation between them remains vague. Hence, two questions remain unsolved in knowledge protection literature concerning the differentiation between resources and capabilities. First, *what exactly are protection capabilities and how do they differ from protection resources*? This question refers to the characteristics of resources and capabilities introduced earlier. Similar to RBV literature, protection resources are also inputs to a production process with protected knowledge as outcome, knowledge capabilities, and protected business strategy. Opposed to that, most knowledge protection literature focuses on protection resources. Intellectual property rights (IPRs) are treated as intangible assets [1], protection related know-how as person-dependent resource [29] technical measures as physical resources [14], HR mechanisms like top management support as person-dependent resources [2] just to mention a few examples. However, on their own, few protection resources are productive. As an example, individual patents do not prevent imitation or substitution in some industries and, hence, firms need build specific combinations of patents, i.e. patent fences to protect their innovations [30]. Another example is that the specific combination of skills makes a product complex and exacerbates imitation by externals [31]. Hence, firms need to build teams of protection resources, specific combinations of coordination between resources and people as well as between people.

The second question is *what do protection capabilities protect?* This question refers to the boundary of protection capabilities, i.e. where they have the power to protect and where protection is beyond their scope. Taking the example from above, the capability of building patent fences strives to protect knowledge embedded in processes and products [3] and, hence, to protect a resource. As protective capabilities are complex patterns of resources and people which hold tacit knowledge, patent fences cannot be considered to protect each type of organizational capabilities as the

protection of tacit knowledge is beyond their scope [3]. This example indicates that the question of what capabilities ought to protect cannot be determined in a general way. To answer this question, ACAP can be used as a reference model to which protection capabilities are mirrored against. Depending on whether externals try to identify, assimilate, or apply knowledge, the focal firm has to protect resources, capabilities, or its business strategy. This is explained in the following. Identifying external knowledge: identifying means observing knowledge which is determined by the extent of disclosure [32] and recognizing its value [33]. Capabilities, however, are not observable as they are invisible phenomena [34]. As a consequence, protection capabilities to reduce the risk of knowledge identification have to focus on knowledge, i.e. the resource level. Assimilating identified knowledge: once identified, externals have to assimilate knowledge of the focal firm, i.e. to embed it into the existing knowledge base. The outcome of assimilation is a new organizational capability [35] as externals try to combine the identified knowledge with their other resources. However, to be able to imitate a capability, the absorbing organization needs to understand causal relationships between the knowledge identified, and other resources and people that constitute the capability. Hence, protection capabilities of firms reducing externals' assimilation capabilities focus on the protection of capabilities. Applying assimilated knowledge: once knowledge has been identified and assimilated, externals need to put it into practice, i.e. to build a business strategy that exploits the assimilated knowledge best by assuring appropriability of returns [10, 23]. In this respect, a focal firm can reduce the risk that externals make use of the imitated capability. Here, protection capabilities operate on protecting a firm's business strategy, by ensuring the appropriability of returns [10, 23].

Using ACAP as a framework, this paper proposes protection capabilities that help firms to reduce the risk of identification, assimilation, and application of their knowledge. These protection capabilities are proposed in the following. Since capabilities are combinations of resources, and since the IT artifact is under-researched in knowledge protection literature [36] there is a stronger focus on what role IT plays in building each of the capability types.

3.2 Concealment, Ambiguity, and Enforcement

Starting from ACAP, this paper argues that firms can reduce the risk that knowledge is identified, assimilated, and applied by establishing concealment, ambiguity, and enforcement capabilities. Figure 1 illustrates the capability model. In the following, the three types of protection capabilities are proposed.

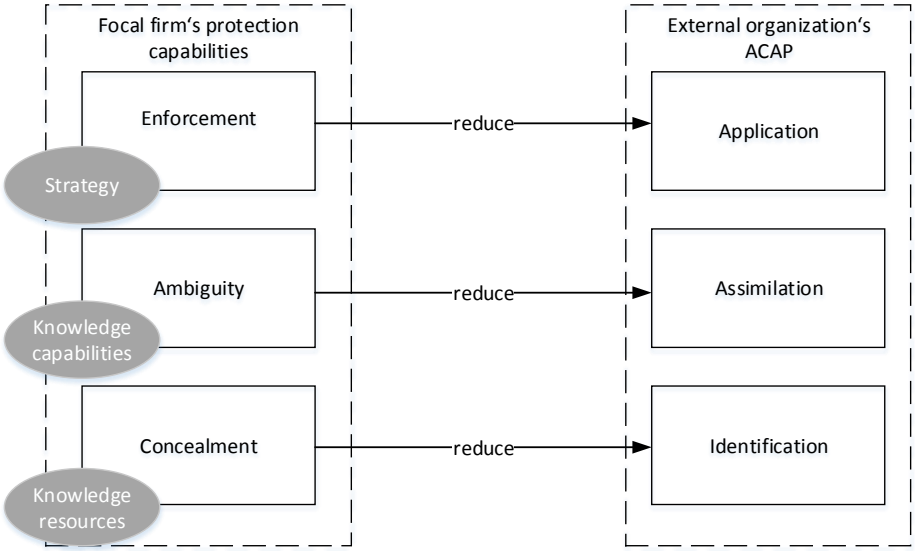

Figure 1: A capability model for knowledge protection

Concealment capabilities: leveraging resources from outside is crucial for organizations due to their limited internal resources [22]. In this respect ACAP postulates that organizations need to develop capabilities to identify external knowledge [11, 26]. More concretely, the observability of knowledge reflects the capability of externals to identify strategic knowledge of a focal firm [37]. Hence, reducing the observability can be understood as reducing externals' capabilities to identify the knowledge. Observability depends on two characteristics: the "extent of disclosure" [32], as well as the ease of "understanding and examining different aspects" of the knowledge [33]. In other words, the success of externals to identify knowledge of a focal firm depends on the level of disclosure and if the knowledge can easily be recognized as valuable. Here, some firms are able to manage to be less transparent or open than others [38]. As a consequence, firms need to learn how to do so and develop protection capabilities that reduce the level of observability [3, 18]. This includes knowledge in people as well as process and product knowledge [39]. The level of disclosure is often determined by technical measures and prominently discussed in information security literature which are well applicable for explicit knowledge [39]. Here, Role-based access control-techniques are proposed for Knowledge Management System (KMS) design [40] which is especially important for inter-organizational workflows [41] and collaborative systems [42]. Another way of IT enhancing firms to reduce observability is (semi-) automation of text sanitization [43]. Together with intentionally using less rich media for transmission for specific cases [8], such technologies provide the capability to hide sensitive knowledge in documents [43] and protect them from externals' observation. However, these measures themselves are no capabilities. Hence, the establishment of routines by combining and coordinating IT resources with people and other protection resources is crucial. One important aspect in this respect is the establishment of routines to increase security awareness to hinder protection measures to be bypassed. Similar to what Roberts et al. [11] describe as developing a shared

ideology towards knowledge transfer, knowledge protection also requires shared language, common goals, or cohesion [29]. A firm needs to establish an adequate level of knowledge protection awareness to ensure that protection measures to reduce disclosure of knowledge can be established. For example, employees might not know what to protect and what not if they are not aware of the firm's competitive knowledge [2]. An example of such a capability that combines and enhances coordinating protection measures to reduce disclosure with people involved in protection processes is a KMS that helps "firstly to store and communicate security related knowledge contents and secondly to allow users to compare their security-relevant activities with security policies, and to either suggest on security policy amendments or additions to training programs" [44].

To reduce the recognition of the value of knowledge, increasing its contextualization is helpful. Contextualization can be understood as the process of embodying explicit knowledge into implicit knowledge [45] and, hence, can be referred to as internalization [46]. In this paper the focus is on internalization within organizational boundaries. Tacit knowledge is deeply rooted in an individual's commitment to a specific context and action [46], and hence it is more difficult for an external observer to recognize the value of tacit than explicit knowledge. That is, because increasing contextualization of knowledge requires an external to have a higher level of prior related knowledge to recognize its value. Prior related knowledge of a firm is the existing domain-specific knowledge base [11]. New knowledge is related to this prior knowledge to be able to be absorbed. Externals with a low level of prior knowledge cannot simply forward tacit knowledge like documents to someone who has a higher level. Although contextualization can be considered as a capability itself [35], combination of routines with IT is of value. Increasing computer-based communication is one solution [47] although it might sound counter-intuitive for a moment. However, it is important to notice that such systems should be established within organizational boundaries and separated from communication channels with externals. To internalize on an organizational level, explicit knowledge has to be shared [46] and integrating internal computer-based communication systems, together with the capabilities to reduce disclosure described above, help to spread explicit knowledge throughout but within the boundary of the organization.

***Ambiguity capabilities**:* as mentioned, assimilation serves to produce new organizational capabilities [35]. ACAP postulates that externals can better assimilate and apply knowledge gained from a focal firm when they have similar resources, e.g. skills, or knowledge [6]. That is because it takes more to assimilate and imitate capabilities than just exposing individuals to new knowledge. One way of reducing the externals capabilities to assimilate is to establish and maintain causal ambiguity. Causal ambiguity describes the nature of causal relationships between actions and results [48] and helps to build barriers to imitation [31]. Increasing causal ambiguity makes it difficult for externals to comprehend the competencies on which certain outcomes are based [31]. Consequently, causal ambiguity protects on the capability level as it exacerbates to understand how different resources and people are combined and coordinated together with the already identified knowledge so that they can imitate the capability. One aspect to increase causal ambiguity is to increase complexity of a firm's competencies, i.e. capabilities themselves [31]. Complexity refers to patterns of "interdependent technologies, routines, individuals, and resources linked to a

particular knowledge" [38]. Increased complexity makes capabilities more difficult to comprehend by externals [10] because "the causes of success and failure are often difficult to assign…[and]…the establishment of cause-effect relationships can be very difficult" [49]. As a consequence, firms need an ambiguity capability that helps to create complex skill patterns, resource deployments [31] as well as complex relationships between capabilities different from the knowledge base of externals. One important factor of complexity is integrating broad-spans of different knowledge-based resources into capabilities [38]. Drawing on the argumentations above, the key to an ambiguity capability is that the focal firm should be able to integrate across the broad-spans of knowledge-based resources to understand the causal relationships [38] whilst externals should not. For the integration part, KMS integrate broad-spans of knowledge helping firms to locate documents, update knowledge elements, coordinate KM tasks etc. [23]. However, firms need to be able to control who is involved in integrative operations in KMS to assure that the complexity of relationships between knowledge-based resources, routines, people etc. cannot be understood by externals. Here, using security concepts like role-based access control or obligation- and condition-based usage control for knowledge management systems [40] is valuable. Firms can control who has access to what and define conditions and obligations underlying an activity that is performed using a KMS. This way, firms can steer who is able to understand the causal relationships in what way.

Furthermore, increasing contextualization of knowledge also helps firms to exacerbate assimilation of knowledge by externals as the decision rules and protocols are hard to codify through "the skilled operator's own level of unawareness" [31]. And, hence, an external cannot fully understand how actions and results relate with increasing tacitness [31]. This relationship between causal ambiguity and contextualization highlights that reducing observability by increasing tacitness of core knowledge also reduces the risk of assimilation.

Enforcement capabilities: ACAP literature proposes that, besides capabilities to identify and assimilate, externals need to be able to apply knowledge which can be achieved by means of inside-out capabilities. In other words, once externals assimilated knowledge and built capabilities therewith, they need to put it into practice, i.e. build a business strategy that exploits the assimilated knowledge best by assuring appropriability of returns [10, 23]. This paper argues that a focal firm needs protection capabilities to reduce the risk that externals apply knowledge. There are basically two ways discussed in literature to protect knowledge after being disclosed and assimilated. Protection (1) via IPR [1, 3] and (2) building trust to prevent externals from opportunistic behaviour [6]. However, trust building implies willingness to form organizational partnerships. Since firms also need to reduce the risk of utilizing knowledge by competitors or even unknown players in the market, the aspect of building trust is neglected here. In terms of IPR, single patents may not prevent imitation or substitution and, hence, firms need build capabilities, i.e. specific routines to establish and maintain patent fences [30]. Here, combining patent fences with IT that supports to manage them is of value. In this respect, property asset management systems or enterprise intellectual asset management systems [50] provide firms with analysis tools, databases, as well as matching algorithms to find similar intellectual properties of externals or incompatibilities between patents of the focal firm.

Another point is that, similar to what ACAP proposes, firms also need to manage dependencies among its various activities to enhance protection, i.e. build an overarching protection strategy [29] to protect the business strategy. A firm's enforcement capability also refers to the establishment of an overarching protection strategy to effectively apply IPR. Drawing from information security literature, firms need to establish IPR requirements, controls to enforce them, as well as auditing procedures [51]. One approach could be seen in the IT architecture proposed by [52]: Adapted to knowledge protection firms should establish links between high-level IPR protection requirements, controls and configurations of property asset management systems or enterprise intellectual asset management systems. Through these linkages, firms can build the capability to measure performance of IPR protection to prevent leaks that could lead to appropriation [18]. By constantly monitoring the compliance status of IPR protection requirements, a firm is able to evaluate the enforcement of protection via IPR. This also enables firms to change or reconfigure their substantive enforcement capabilities [cf. 11]. Helpful in this respect could be technologies that enable continuous auditing, e.g., by using a process mining approach for constantly checking for compliance [53].

4 Discussion

Knowledge protection literature mainly focuses on the effectiveness of applying measures in a generalized way, widely ignoring abilities of individual firms in how they can build capabilities around the measures. Drawing on the RBV, this paper addresses this problem presenting a model that (1) proposes three types of protection capabilities. (2) This paper argues how these protection capabilities help to reduce the risk that knowledge is identified, assimilated, and utilized. (3) This paper differentiates between the levels on which protection capabilities operate: protecting resources, capabilities, or the business strategy of a focal firm. Concerning (1) this paper goes beyond current knowledge protection literature as it clearly distinguishes between the concepts of resource and capability and provides concealment, ambiguity, and enforcement capability types. Concerning (2) the model considers peculiarities of individual firms by the fact that the firms' own protection capabilities are mirrored against the ACAP of individual external organizations. Here, concealment help to reduce the risk to identify knowledge, ambiguity to reduce assimilation, and enforcement to reduce application. Concerning (3) the paper anchors the concept of protection capabilities in the RBV by arguing that concealment capabilities protect knowledge resources, ambiguity capabilities protect knowledge capabilities, and enforcement capabilities protect the business strategy of a firm.

4.1 Implications

Managerial implications: First of all firms might rethink their approach to knowledge protection. Although, many firms do not have knowledge protection on their radar [54], those who do should not consider protection solely as application of measures [cf. 29] but rather as a set of capabilities. Firms could ask themselves "what

protection capabilities do we need to protect our knowledge, our capabilities and our business strategy", "how can we build, or enhance these capabilities", or "how do we have to reconfigure them depending on the ACAP of externals". In the course of this firms might think of how IT resources can be used to build protection capabilities. Here, they can consider the use of new technology enhancing capabilities like KMS that incorporate user knowledge on security awareness [44].

Research implications: There are several implications for research from introducing this capability model. First of all, this paper tries to highlight the need to sharpen the different concepts of resources and capabilities. Protection resources themselves often fail to adequately protect [30], whilst their combination with other protection resources help firms to deal with externals' ACAP. This leads to the second point: this paper tries to shift the focus in knowledge protection literature from the application of protection resources to their combination and utilization as protection capabilities. This enables to consider the peculiarities of individual firms and, hence, helps them to balance sharing and protecting. This so called boundary paradox [6, 9] refers to the need of firms to access external knowledge due to limited resources and protect internal knowledge. Recently, no literature provides solutions to solve it.

4.2 Boundaries of the research and further research

It is necessary to explicate the boundaries of this conceptual paper as there are some limitations to the explanatory power and comprehensiveness of the model.

Explanatory power of the model: This model makes no statements on the extent to which the capabilities can reduce identification, assimilation, and application. In this respect, further studies need to investigate the influential strength of the capabilities on (1) externals' ACAP and (2) the focal firm's overall protection performance. With respect to (1) no work could be found that makes statements thereon and, hence, further exploratory studies are of importance. For (2), literature indicates that to a certain extent, contextualization can even be effective "for resolving comprehension difficulties arising from the users' lack of task domain knowledge" [55]. Similarly, a too high level of causal ambiguity leads to a situation where even employees of the focal firm do not understand how actions and outcomes relate [31]. Further studies need to investigate the relationships of concealment, ambiguity, and enforcement capability with a firm's protection performance and associated coordination costs. Furthermore, the model makes no statements on the relationships between the capabilities themselves. As indicated, the level of contextualization positively influences causal ambiguity [38]. Hence, it is reasonable to assume that concealment capabilities affect ambiguity capabilities. In other words, firms that increase tacitness of knowledge might also increase causal ambiguity. Further studies should also investigate how concealment and ambiguity capabilities relate to enforcement capabilities.

Comprehensiveness of the model: The paper does not claim that the proposed set of capability types is comprehensive. It might occur in further studies that there are more than three types of capabilities reducing the ACAP of externals. Additionally the IT resources are of exemplary character. Due to the fact that the IT artifact is mainly absent in knowledge protection literature [36] it might be of value to perform

deeper investigations on which IT might contribute in what way to the three capability types.

References

1. Hertzfeld, H.R., Link, A.N., Vonortas, N.S.: Intellectual Property Protection Mechanisms In Research Partnerships. Research Policy 35, 6, 825-838 (2006)
2. Norman, P.M.: Are Your Secrets Safe? Knowledge Protection in Strategic Alliances. Business Horizons 44, 6, 51-60 (2001)
3. Liebeskind, J.P.: Knowledge, Strategy And The Theory Of The Firm. Strategic Management Journal 17, Winter Special Issue, 93-107 (1996)
4. Amara, N., Landry, R., Traoré, N.: Managing the protection of innovations in knowledge-intensive business services. Research Policy 37, 9, 1530-1547 (2008)
5. Brouwer, E., Kleinknecht, A.: Innovative output, and a firm's propensity to patent.: An exploration of CIS micro data. Research Policy 28, 6, 615-624 (1999)
6. Norman, P.M.: Protecting Knowledge In Strategic Alliances: Resource And Relational Characteristics. The Journal of High Technology Management Research 13, 2, 177-202 (2002)
7. Ford, D.P., Staples, S.: Are full and partial knowledge sharing the same? Journal of Knowledge Management 14, 3, 394-409 (2010)
8. Bloodgood, J.M., Salisbury, W.D.: Understanding the influence of organizational change strategies on information technology and knowledge management strategies. Decision Support Systems 31, 1, 55-69 (2001)
9. Jordan, J., Lowe, J.: Protecting Strategic Knowledge: Insights From Collaborative Agreements In The Aerospace Sector. Technology Analysis & Strategic Management 16, 2, 241-259 (2004)
10. Grant, R.M.: The resource-based theory of competitive advantage: implications for strategy formulation. Knowledge and Strategy.(Ed. M. Zack) pp 3-23 (1991)
11. Roberts, N., Galluch, P.S., Dinger, M., Grover, V.: Absorptive Capacity and Information Systems Research: Review, Synthesis, and Directions for Future Research. MIS quarterly 36, 2, 625-648 (2012)
12. Baughn, C.C., Denekamp, J.G., Stevens, J.H., Osborn, R.N.: Protecting Intellectual Capital In International Alliances. Journal of World Business 32, 2, 103-117 (1997)
13. Gold, A.H., Malhotra, A., Segars, A.H.: Knowledge Management: An Organizational Capabilities Perspective. Journal of Management Information Systems 18, 1, 185-214 (2001)
14. Desouza, K.C., Vanapalli, G.K.: Securing knowledge in organizations: lessons from the defense and intelligence sectors. International Journal of Information Management 25, 1, 85-98 (2005)
15. Manhart, M., Thalmann, S.: Protecting Organizational Knowledge: A Structured Literature Review. to appear in Journal of Knowledge Management 19, 2, (2015)
16. Ahmad, A., Bosua, R., Scheepers, R.: Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective. Computers & Security 42, May, 27-39 (2014)
17. Jennex, M., Durcikova, A.: Assessing Knowledge Loss Risk. In: 46th Hawaii International Conference on System Sciences, HICSS46. IEEE Computer Society, (Year)
18. Lee, S.C., Chang, S.N., Liu, C.Y., Yang, J.: The Effect of Knowledge Protection, Knowledge Ambiguity, and Relational Capital on Alliance Performance. Knowledge and Process Mgmt 14, 1, 58-69 (2007)

19. Ilvonen, I.: Knowledge Security-A Conceptual Analysis. . vol. PhD Thesis. Tampere University of Technology (2013)
20. Kale, P., Singh, H., Perlmutter, H.: Learning and protection of proprietary assets in strategic alliances: building relational capital. Strategic Management J 21, 217-237 (2000)
21. Amit, R., Schoemaker, P.J.: Strategic assets and organizational rent. Strategic management journal 14, 1, 33-46 (1993)
22. Trkman, P., Desouza, K.C.: Knowledge Risks in Organizational Networks: An exploratory Framework. Journal of Strategic Information Systems 21, 1-17 (2012)
23. Maier, R.: Knowledge Management Systems: Information And Communication Technologies For Knowledge Management. Springer, Berlin (2007)
24. Winter, S.G.: Understanding dynamic capabilities. Strategic management journal 24, 10, 991-995 (2003)
25. Zahra, S.A., George, G.: Absorptive Capacity: A Review, Reconceptualization, and Extension. The Academy of Management Review 27, 2, 185-203 (2002)
26. Cohen, W.M., Levinthal, D.A.: Absorptive capacity: a new perspective on learning and innovation. Administrative science quarterly 128-152 (1990)
27. Wade, M., Hulland, J.: Review: the resource-based view and information systems research: review, extension, and suggestions for future research. MIS quarterly 28, 1, 107-142 (2004)
28. Fosfuri, A., Tribó, J.A.: Exploring the antecedents of potential absorptive capacity and its impact on innovation performance. Omega 36, 2, 173-187 (2008)
29. Olander, H., Hurmelinna-Laukkanen, P., Heilmann, P.: Do SMEs Benefit From HRM-Related Knowledge Protection In Innovation Management? International Journal of Innovation Management 15, 3, 593-616 (2011)
30. Cohen, W.M., Nelson, R.R., Walsh, J.P.: Protecting their intellectual assets: Appropriability conditions and why US manufacturing firms patent (or not). National Bureau of Economic Research (2000)
31. Reed, R., Defillippi, R.J.: Causal Ambiguity, Barriers To Imitation, And Sustainable Competitive Advantage. The Academy of Management Review 15, 1, 88-102 (1990)
32. Winter, S.G.: Knowledge and competence as strategic assets. In: Teece, D.J. (ed.) The Competitive Challenge: Strategies for Industrial Innovation and Renewal, pp. p.159-184. Ballinger, Cambridge, MA (1987)
33. Zander, U.: Exploiting a technical edge: voluntary and involuntary dissemination of technology. (1991)
34. Itami, H., Roehl, T.W.: Mobilizing invisible assets. Harvard University Press (1991)
35. Harvey, M.G., Speier, C., Novicevic, M.M.: The impact of emerging markets on staffing the global organization:: A knowledge-based view. Journal of International Management 5, 3, 167-186 (1999)
36. Pawlowski, J.M., Bick, M., Peinl, R., Thalmann, S., Maier, R., Hetmank, L., Kruse, P., Martensen, M., Pirkkalainen, H.: Social Knowledge Environments. Business & Information Systems Engineering 6, 2, (2014)
37. Bou-Llusar, J.C., Segarra-Ciprés, M.: Strategic knowledge transfer and its implications for competitive advantage: an integrative conceptual framework. Journal of Knowledge Management 10, 4, 100-112 (2006)
38. Simonin, B.L.: Ambiguity and the process of knowledge transfer in strategic alliances. Strategic Management Journal 20, 7, 595-623 (1999)
39. Desouza, K.C.: Knowledge Security: An Interesting Research Space. Journal of Information Science and Technology 3, 1, 1-7 (2006)

40. Bertino, E., Khan, L.R., Sandhu, R.: Secure Knowledge Management: Confidentiality, Trust, And Privacy. IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans 36, 3, 429-438 (2006)
41. Kang, M.H., Park, J.S., Froscher, J.N.: Access control mechanisms for inter-organizational workflow. In: Proceedings of the sixth ACM symposium on Access control models and technologies, pp. 66-74. ACM, (Year)
42. Tolone, W., Ahn, G.-J., Pai, T., Hong, S.-P.: Access control in collaborative systems. ACM Computing Surveys (CSUR) 37, 1, 29-41 (2005)
43. Sánchez, D., Batet, M., Viejo, A.: Minimizing the disclosure risk of semantic correlations in document sanitization. Information Sciences 249, 110-123 (2013)
44. Lupiana, D.: Development of a framework to leverage knowledge management systems to improve security awareness. (2008)
45. Yang, B.: Toward a holistic theory of knowledge and adult learning. Human Resource Development Review 2, 2, 106-129 (2003)
46. Nonaka, I.: The knowledge-creating company. Harvard business review 69, 6, 96-104 (1991)
47. Becerra-Fernandez, I., Sabherwal, R.: ICT and knowledge management systems. In: Schwartz, D.e. (ed.) Encyclopedia of Knowledge Managament, pp. 230-236. Idea Group Inc., Hershey, PA/ London (2006)
48. Lippman, S.A., Rumelt, R.P.: Uncertain imitability: An analysis of interfirm differences in efficiency under competition. The Bell Journal of Economics 418-438 (1982)
49. Barney, J.B., Ouchi, W.: Information cost and the governance of economic transactions. Organizations and markets 347-372 (1985)
50. Dou, H., Leveillé, V., Manullang, S., Dou Jr, J.M.: Patent analysis for competitive technical intelligence and innovative thinking. Data science journal 4, 209-236 (2005)
51. Hong, K.-S., Chi, Y.-P., Chao, L.R., Tang, J.-H.: An integrated system theory of information security management. Information Management & Computer Security 11, 5, 243-248 (2003)
52. Thalmann, S., Bachlechner, D., Demetz, L., Manhart, M.: Complexity is dead, long live complexity! How software can help service providers manage security and compliance. Computers & Security 45, 172-185 (2014)
53. Thalmann, S., Manhart, M., Ceravolo, P., Azzini, A.: An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection. International Journal of Knowledge Management 10, 2, (2014)
54. Jennex, M., Olfman, L.: Assessing knowledge management success. International Journal of Knowledge Management 1, 2, 33-49 (2005)
55. Mao, J.-Y., Benbasat, I.: Contextualized access to knowledge: theoretical perspectives and a process-tracing study. Information Systems Journal 8, 3, 217-239 (1998)