THE ENDS OF KNOWLEDGE SHARING IN NETWORKS: USING INFORMATION TECHNOLOGY TO START KNOWLEDGE PROTECTION

Complete Research

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

Stefan Thalmann, University of Innsbruck, Innsbruck, Austria, stefan.thalmann@uibk.ac.at

Ronald Maier, University of Innsbruck, Innsbruck, Austria, ronald.maier@uibk.ac.at

Abstract

Organisations need networks to leverage external knowledge, particularly for SMEs with their limited resources. Organisations use networks for knowledge sharing to foster innovation. This use of networks bears risks like the unwanted spill-over of knowledge. Consequently, organisations need to balance sharing and protecting knowledge. While scholars have extensively investigated the sharing perspective, they have so far neglected knowledge protection in network settings and especially the interplay between sharing and protection. This paper illuminates the motives and practices of network members switching from open sharing to stronger protection on the basis of 53 interviews with members from 10 SME networks. We describe three patterns of switching behaviour and explain how the interviewees adapt the use of collaborative IT to manage the switches. Employees switch from sharing to being open to (a) a certain extent, (b) a certain group, or (c) a certain topic. We find that the three types of switching behaviour are related to network characteristics and to corresponding adaptions in using collaborative IT. Collaborative IT does not necessarily hamper knowledge protection, but adapted use can support both knowledge sharing and knowledge protection. We argue that organisations should develop protection capabilities to manage the switches.

Keywords: knowledge protection, knowledge sharing, networks, collaborative IT.

1 Introduction

Networks are forms of collaboration between organisations that become more and more important for firms to acquire knowledge (Trkman and Desouza, 2012). Sharing and collaboratively developing knowledge in networks is highly important since individual firms and particularly small and medium-sized enterprises (SME) have limited resources to leverage knowledge (Easterby-Smith et al., 2008, Wagner and Bukó, 2005). The use of collaborative information technology (IT) in networks has grown since it provides expanding opportunities for knowledge sharing (Trkman and Desouza, 2012). Sharing is one of the most important purposes, if not the raison d'être of networks. However, there are also risks for organisations sharing knowledge in networks, such as the unwanted spill-over of competitive knowledge to competitors which has not only detrimental effects for the affected member, but also for the whole network because it can hinder knowledge sharing (Trkman and Desouza, 2012). Empirical evidence shows that practitioners still hardly pay attention to the protection of knowledge, though (Jennex and Durcikova, 2014).

While scholars have extensively investigated knowledge sharing or transfer in networks (e.g., Tsai, 2001, Wagner and Bukó, 2005) and its IT support (e.g., Lertpittayapoom et al., 2007, Roberts, 2000), little attention has been paid to the protection of knowledge in networks. The few scholars that investigated topics related to knowledge protection on the network level focused on the identification of knowledge risks in networks (Trkman and Desouza, 2012) or risks for organisations imposed by social media (Väyrynen et al., 2013). Further, IT artefacts to manage protection have hardly been studied (e.g., Bertino et al., 2006). However, networks are only viable as long as their members are willing to share and jointly develop knowledge and this requires that members can also protect their competitive knowledge. Therefore, we need to better understand how members of networks address the tension between sharing and protection.

We address this research gap by investigating how network members switch from being open towards being protective on the basis of 53 interviews with members from 10 SME networks. We describe three patterns with episodes of switching and explain how the interviewees adapted collaborative IT for this purpose. In section 2, we introduce the concepts that build the basis for our study, i.e. knowledge sharing and knowledge protection. Section 3 explains the procedure of our study. We describe the interview sample and the methods we applied for data collection and analysis. Section 4 presents the results, i.e., the network descriptions and the three switching patterns. We discuss our findings in section 5 and provide a conclusion and an outlook on further research in section 6.

2 Related Work

"Knowledge transfer in organisations is the process through which one unit is affected by the experience of another" (Argote and Ingram, 2000). Several hurdles appear when we intend to transfer knowledge across different contexts (Argote and Ingram, 2000). Difficulties in absorbing knowledge increase with a decreasing contextual linkage between receiver and knowledge (Reagans and Mcevily, 2003). Thus, the transferability and absorbability of knowledge highly depends on the receiver's characteristics (Bou-Llusar and Segarra-Cipre´S, 2006). Sharing in networks has the advantage that the characteristics of the knowledge sender and receiver are similar to a certain extent, which facilitates the knowledge transfer. Organisations engaged in networks assumedly better understand the requirements of their partners and thus prepare knowledge in such a way that the effort for adapting it for other member organisations is reduced (Malhotra et al., 2005, Lin et al., 2012). Different network structures represent different opportunities for a member organisation to access new knowledge (Tsai, 2001) but also to loose knowledge by accident.

Knowledge protection is an important contributor to successful knowledge management (Jennex and Zyngier, 2007) and concerns the prevention of (a) unwanted knowledge spill-overs (Ahmad et al., 2014), (b) knowledge loss (Jennex and Durcikova, 2013), and (c) the reduction of knowledge visibility (Lee et al., 2007). (a) focuses on leaking knowledge to unauthorised people, (b) deals with leaving or retiring employees, and (c) is concerned with observability of knowledge by externals. Previous research showed that SMEs often do not have the resources to implement formal protection measures such as patents and trade secrets and therefore rely more on informal protection measures (Leiponen and Byma, 2009, De Faria and Sofka, 2010). The risk of knowledge spill-overs is typically addressed through secrecy or complex design (De Faria and Sofka, 2010). However, SMEs perceive secrecy not as a very effective strategy (Leiponen and Byma, 2009).

Knowledge protection literature mostly fails to consider the IT artifact as it originates in the research field of strategic management (Manhart and Thalmann, 2015). Most knowledge protection literature has a nominal view on the IT artifact, considering it as absent although used incidentally or as background information (e.g., Kale et al., 2000, Arundel, 2001). Analyzing how SMEs use IT to protect their knowledge can be a starting point to address this gap. Knowledge sharing in networks has been investigated in terms of influencing factors (Wagner and Bukó, 2005) or risks (Trkman and Desouza, 2012) but has not yet described the motives and practices of switching between sharing and protection, particular in network settings. Further, knowledge protection literature also stresses the need for finding a balance between sharing and protecting knowledge without having a solution so far (Thalmann et al., 2014). Scholars propose frameworks to balance sharing and protecting (e.g., Baughn et al., 1997), however, there is still limited knowledge on how organisations try to manage this balance especially under the light of emerging social software (Manhart and Thalmann, 2015). Further, a large part of literature on knowledge protection focuses on the effective application of formal or informal measures (Hertzfeld et al., 2006, Thalmann and Manhart, 2013). However, organisations need to consider their protective capabilities to achieve and sustain competitive advantage (Andersén, 2012).

We follow the scholarly call for more research on knowledge protection in networks by recommending to explore the use of IT, to focus also on informal networks (Manhart and Thalmann, 2015), to focus on knowledge protection in social knowledge environments (Pawlowski et al., 2014)

3 Procedure

The goal of our study is to investigate how members of networks strike a balance between sharing and protecting knowledge by means of switching from open sharing to stronger protection. We collected data by means of semi-structured interviews. We interviewed several members of each network in order to obtain a multi-perspective view on the knowledge protection behaviour in the network. We asked the individuals to describe their personal sharing and protection behaviour acting as representatives of their organisations. Therefore, our unit of analysis is the individual representing an organisation that is member of one or many networks.

We conducted 53 semi-structured interviews with employees from the member organisations of ten SME networks in construction, healthcare, IT, and engineering between January and October 2014. We conducted the interviews in the scope of the LEARNING LAYERS research project, which focuses on IT support for informal learning.The networks and key informants were selected based on convenience sampling and the networks are affiliated to the research project. We organised our study in two phases. First, we interviewed ten key informants who occupied a central role in the network, e.g., network management, and had a good overview of the network members and activities. The key informant interviews took approximately two hours and were conducted face to face. The goal was to get a first overview of the networks and to identify promising candidates for the subsequent informant interviews. Each key informant represented one of the ten SMEs organised in one of the investigated networks from Germany or Austria. Second, we conducted 43 informant interviews with members identified by the key informants of each network. We interviewed between three and five informants in each of the 10 networks to gain a deeper understanding of each network and to create a multi-perspective view on the interplay between sharing and protection in the networks. The informant interviews took approximately one hour each and were conducted via telephone. We allowed for the interviews to build on each other, complement, challenge and extend intermediate findings from interview to interview to develop our understanding and theorising. Seven interviewees had less than five years, 46 had more than five years of working experience with the network which indicates that most interviewees had profound experience with the networks. Table 1 provides a description of the investigated networks (sector, number of member organisations) and the number of performed interviews.

Network (ID)	Sector	# Member orgs.	# Interviewees
Network 1	Construction	130	6
Network 2	Construction	30	6
Network 3	Construction	92	5
Network 4	Construction	270	6
Network 5	Construction	1600	6
Network 6	Construction	85	5
Network 7	Information Technology	108	5
Network 8	Health	63	6
Network 9	Engineering	83	4
Network 10	Health	139	4

Table 1. Overview of the investigated networks

The audio-recorded interviews were transcribed verbatim and cleansed afterwards. Thereby, the raw transcripts were checked for accuracy. Additionally, this procedure helped us to get familiar with the data material, as not all of us were involved in the data collection to the same degree. Transcriptions were translated into English for citing original voice. We analysed the transcripts by applying an informed inductive coding procedure, carried out via Atlas.ti.

We strived to identify categories from the material itself, not from theoretical considerations (Mayring, 2014). In line with the inductive category development according to Mayring (2014), we firstly defined a criterion for the selection process in category formation as a deductive element within our analysis. That is, we defined the dimensions of analysis (collaborative IT, protection behaviour, network characteristics). One author initially scanned 20% of the data material and proposed eight initial codes according to these dimensions of analysis. As an example, for collaborative IT “already used IT” and “desired IT” was proposed as codes. In parallel, we created a coding table with descriptions of the initial codes, an example, and rules for applying the codes. Based on this table, we started the first collaborative analysis round focusing on three to five transcripts each. Each team member focused on the assigned transcripts covering one network using the table describing the initial eight codes. During this phase the initial codes were refined and new codes proposed by each team member. All codes in the sample were discussed and clarified in a subsequent discussion round. We did not calculate a value for the inter-coder reliability, however, we performed this routine until we had an agreement upon the sample of codes and their use amongst the three coders. We found no additional codes for ‘collaborative IT’ and ‘network characteristics’, the dimension protection behaviour was changed to ‘switching behaviour’ and three additional codes. Two codes for network characteristics were rejected. All in all, we agreed upon the following codes on text passages (in brackets quantity of use of this code): collaborative IT: “already used IT” (387), “desired IT” (100). Protection behaviour: “open to a certain group” (78), “open to a certain topic” (303), and “open to a certain extent” (47). Network characteristics: “geographic proximity” (141), “professional proximity” (98). Subsequently, we started a second round of coding where we coded the entire data set using the new set containing eleven codes. After that, we discussed all coded text passages to have a full agreement on the codes and their use and started with the interpretation of the data (Mayring, 2014).

4 Switching Patterns

In this section, we first categorise the networks we investigated with the help of the two dimensions geographic proximity and professional proximity. We then go on to describe three switching patterns from knowledge sharing to knowledge protection and also illuminate how network members adapt their use of collaborative IT to be protective.

4.1 Network Description

The networks in our sample differ in their geographic reach. A high geographical proximity refers to the same local co-presence of network members (Schamp et al., 2004), i.e. they have their locations next to each other. We found that the networks in our sample differ in terms of geographical proximity. They are either bound to a specific region or they are regionally unbounded. We classified our networks according to the network demographics collected during the interviews and by investigating available reports describing the networks. The geographic and the professional (business domain) are the two most prominent proximity dimensions we came across in our data analysis.

The networks also differ in terms of the professional heterogeneity of their members. We characterise a network as heterogeneous if its member organisations come from different professional domains or occupy different roles in the supply chain. We characterise networks as homogeneous if their members come from the same or similar professional domains and occupy the same or similar roles in the supply chain. We analysed membership lists of each network to identify their roles in the supply chain and to determine their professional domains.

Comparing our networks according to their members' geographical and professional proximities, we identified four types of networks (see Table 2).

	Regionally unbounded	Regionally bounded
Homogeneous		N3, N4
Heterogeneous	N1, N5	N2, N6, N7, N8, N9, N10

Table 2. Geographical and professional proximities of the investigated networks

We acknowledge that there are more dimensions for characterising networks like cognitive or institutional proximity (Boschma, 2005), however, we focus on the two characteristics described here as they were the only ones we found sufficient empirical evidence for categorising our networks.

Eight out of ten networks are regionally bounded and the majority of our sample of ten networks consists of six heterogeneous, regionally bounded networks (N2, N6-10). This means a large part of our sample consists of networks where the members occupy different roles in the supply chain, work in different domains, and are located in a specific region. Further, the sample contains two homogeneous, regionally bounded networks (N3, N4), and two heterogeneous, regionally unbounded networks (N1, N5). Finally, we have no homogenous, regionally unbounded network in our sample.

4.2 Open to a certain extent

Being open to a certain extent describes episodes where members switched from open sharing to hiding the details of knowledge. Many interviewees reported about the need to be open to innovate (N1-d): "if somebody has a problem with handing on their knowledge, then that is wrong […] this is a mutual give and take situation". We identified that the reluctance to actively contribute, the fear of imitation, and the fear of recourse makes members switch from sharing to being open to a certain extent.

Reluctance to actively contribute: Interviewees highlighted that open sharing suffers from an increasing reluctance of members to actively contribute. Some network members actively absorb without sharing their own knowledge and, thus, giving and taking is thrown out of balance (N5-e): "Well, put in a nutshell, I must say that sucking professional knowledge, to define it that way, has gotten progressively worse in the last years". Another interviewee reported (N1-f): "Our members can present their projects at our meetings. They can show what they did, what went bad, what went good. They can discuss about that. These opportunities have not been taken up extremely well, though". We found that, as a consequence, active members stopped the open sharing to prevent being exploited. They started to share only high-level knowledge with all members of the network and only provide detailed knowledge to members who are willing to compensate (N5-e): "why do I participate as a craftsman, do I just want to waste time or do I want to get an order"? Compensation in this case can be to sign a contract.

We found that network members started to use collaborative IT differently in such situations. First, the distribution of detailed knowledge in threads or blogs has been stopped in N5 and interested members are invited into using synchronous IT collaboration. This way, members want to regain control about who is getting detailed knowledge (N5-e): "Then, I wrote [in the forum] 'if you have further questions, please call me and contact me directly'". Second, the members established subgroups within the network to better coordinate which details of the knowledge should be shared. Hence, some members stopped appearing as an individual, but as a coherent group in the network (N5-e): "the people use a highly professional platform that really offers a gigantic pool of knowledge in the form of pictures, in the form of comments and also links. And the people really are like that today, thrifty is nifty'[…] I don't want to pay […] Therefore, it is good to create a group as we did […] and then the webmaster has placed the links of this team into the platform […] and so we develop a symbiosis in which one pulls the other and gets the thing closer to the target […] we can present the team in a self-contained way and share exactly the knowledge that we would like to share". By forming a group-appearance, members can better control the detail of knowledge to be provided to other members by making arrangements restricted to group members. Acting as individuals, they are not aware about how much details other members might share. If other members share more details, the passive knowledge absorbers might make contracts with members that provide more detailed knowledge.

Fear of imitation: We identified that network members restrict their sharing behaviour due to regular on-site meetings where potential competitors participate. Members offer on-site workshops to distribute knowledge and to spread the ideas of sustainable construction. The context to understand the shared knowledge seems crucial in this respect (N1-a): "Somebody who [tries something] in a seminar, they can apply nothing in real. If somebody would get how that is done at the real construction site, then they would have the self-confident feeling of 'Aha! This is what I have to do or to consider or to know". Rich context seems important for effective knowledge sharing since there is no general rule on how to apply the knowledge, it always depends on the context. This, however, implies that the knowledge is sticky and cannot be easily verbally shared and transferred to other contexts. In other words, participants will learn how to do things in a specific context, but not necessarily how to translate this into their own context. This would require additional de-contextualised knowledge on how to apply knowledge in other contexts. We found that members restrict their sharing at exactly that point. They verbally share knowledge and protect documented knowledge (N1-a): "Well, demonstrating and storytelling are completely open. […]. An architect's drawing or the complete set of documentation would represent so-to-say the inherent value that the architect sells and we never hand this on in that sense". This separation between an open verbal expression of detailed knowledge and a restriction of sharing it in explicit form enables members to share their experiences without disclosing de-contextualised knowledge. We found that members adapt their use of collaborative IT to serve this purpose. For example they use dedicated Dropbox-groups to protect documented knowledge (N1-f): "We have many things in different Dropbox workspaces with different people at the moment […]. There is one Dropbox for the executive board. […] There is a Dropbox for training and education, one for the interns, one for registration, one for our guidelines. Different people take part in these, depending on who contributes and so".

Fear of recourse: Another reason why members restrict their open sharing is that they fear recourses due to sharing knowledge with a low maturity or with missing legal proof (N1-f): "We just want to make sure that we as [network] cannot be held liable for people who are listed on our homepage who do something wrong or deal with some construction tasks inappropriately". However, we found that this fear does not only have an effect on who is listed as a network member on the homepage, but that this also directly affects how members use forums or homepages for sharing knowledge. Although the forum was initiated for open sharing of knowledge, members share general high level knowledge which is mature and reliable, but stop sharing innovative, new and not validated knowledge via traceable IT (N1-e): "I cannot simply write into the forum 'Hey guys, you can put tiles on clay. Then, this cannot be done for whatever reason or somebody forgets the foil or what not. Nobody takes the liberty to accept responsibility. That is the reason you do not find anything there. Therefore, one has to take on that responsibility for oneself". Consequently, members can find general high-level knowledge on the homepage and merely use it as a platform to retrieve information but not to actively share as they only dare to verbally discuss their opinions. As a consequence, members only find high-level information on the homepage (N1-e): "I can discuss about such things, but I cannot just search the Internet or the homepage or some presentation, does this work or does it not. Because there is no rule. There are opinions instead".

4.3 Open to a certain group

Being open to a certain group describes episodes where members switched from open sharing to only sharing to a limited sub-group of the network. We found that the local context of networks has implications on the willingness to share. We found that the extent to which members share knowledge strongly depends on the type of collaboration partner (N8-a): "I do not see any restrictions in offering the know-how that we produce and that we have [in the local] context. Thinking this from the other side, from industry, it is completely different. This is understandable. They have internal know-how which is a much more strategic asset than what we have".

Difficulty to enforce legal measures: Due to the highly competitive situation paired with the willingness to openly innovate, network members establish more formal forms of collaboration based on contracts. However, they experience the challenge of limited control over the knowledge due to the different types of partners in a collaboration and difficulties in enforcing protection by legal measures (N8-a): "It is very, very difficult in [our context] to organise this for ourselves. The difficulty begins with, the question is if they ask us [about a non-disclosure agreement] then we go 'Aha', they say ok, what we hand on to you is of value to us, so please take care of it. The question is and that is what you need to ask as a [occupation] do we have the structures and resources to take care of it? We have a fileserver which is not protected, if it is about electronic documents. We do not have encrypted emails. We have no right as employees to sign such [a non-disclosure agreement]. This must be done by the executive board. The executive board […] eventually cannot take the internal responsibility to establish such a process so that they could sign this in good faith". Another interviewee reported (N10-a): "I was advised according to patent law and the consultant said that I would not be strong enough to enforce a patent […] to execute this. […] I would not be financially strong enough to enforce this against relevant partners even when it was justified". These situations show that the enforcement via legal measures is difficult. The success depends on the capabilities of members to be able to enforce the rules.

We found that member organisations use collaborative IT to circumvent this difficulty of enforcing legal measures in their subgroups (N8-b): "For example, we have developed a tool for IPR [intellectual property rights] in which every publication, every presentation must be uploaded to the Web and there is a time period for objections by [group members] and functionality for commenting. So that publications are revised until all agree and this may be published eventually". Using a tool for managing a release process for IPR-relevant documents helps the partners replace contractual agreements by a more collaborative and ad-hoc approach of finding an agreement on what to share and what not. Then, this allows the formation of larger subgroups in which the enforcement can be checked by IT.

Uncertainty about collaboration partners' sharing behaviour: Members experience uncertainty about their collaboration partners' sharing behaviour. Here, members form subgroups in which they share competitive knowledge but protect it from other members outside the group (N7-a): "We have our group of interest that we co-founded. We have restrictions for it and clear guidelines about how to handle information from outside and on the other side of course how to handle things we develop. Guidelines about how we handle knowledge that we developed". Network management helps groups to determine sharing and protection behaviour of group members to outsiders.

Network management implements communication rules and, therefore, acts as a membrane between the network members, as an enforcer (N10-b): "If somebody says 'this knowledge is confidential' this has to be clarified ex ante. […] When somebody presents an innovation during a project meeting, a NDA circles in this round. I like to keep things amongst the people that sit around the table". This way, network management supports members by forwarding knowledge in a "target-member-specific" way (N7-d): "We send presentations upon request, not in the sense of a newsletter, so that everybody gets everything, but specifically […] so that we ask the creator or owner of the presentation, can we share this, or may we hand this on to this person or that person […] or we get a reduced set of slides which we can distribute or share on our Web site […] that we simply always have four eyes, at least the four-eyes principle, and say is this ok that we share this. Not simply, 'there is something on the fileshare. That is an interesting slide. I hand it on now'". Without using the "four-eye-principle", a presentation might be unintendedly shared with competing members as there are no IT-based restrictions in place. By acting as a membrane, the role of the network management is to keep the members aware of with whom they want to share certain knowledge. This episode exemplifies a switch to sharing behaviour that supports both, knowledge sharing ("if I share it personally, I know that it is taken up") and knowledge protection ("if I share it personally, I know by whom it is taken up"). Interviewees also highlighted the importance of building trust within subgroups (N6-e): "how good do I know somebody? If I know and can take a measure of that person, have many things in common, I can better evaluate whether I can share with that person or not". In this regard, IT seems important to increase trust (N6-d): "I always wished for a tool that strengthens the community […] the general challenge is to establish a basis of trust. If a member wants information to be treated as confidential they should know that a partner treats information confidential".

We found that the network management can provide communication platforms for fostering knowledge transfer. However, due to the uncertainty about the sharing behaviour, sharing becomes rather superficial in N9 while detailed knowledge is only shared personally when members trust each other (N9-d): "Of course, what we also offer […] is our data base of competencies. Every network wants such a data base. This would be a Facebook of [industry sector]. There I go. I can build communities. I can send data back and forth. However, […] it is, as said before, always the personal contacts. That is how we generate projects. If it gets more superficial, we can work with such data bases of competencies".

4.4 Open to a certain topic

Being open to a certain topic describes episodes where members switched from sharing their knowledge to sharing only knowledge about a certain topic.

Some networks have other foci than knowledge sharing for innovation like sharing knowledge to achieve compliance to laws, and are restrictive towards collaboratively developing innovations. Interviewees indicated that originally such networks had also experienced a more open sharing culture which, however, changed. One interviewee demonstrated this change using the example "topping-out ceremony" in the construction industry (N4-f): "Formerly this was the topping-out ceremony. The crafts became better because they all sat together during the topping-out ceremony after a building was completed. […] the only opportunity to exchange informal knowledge and informally learn across the crafts. Unfortunately, this topping-out ceremony doesn't exist anymore in this fashion. Hence, a central aspect of informal learning has disappeared on this level".

The openness for sharing focuses on exchanging knowledge that is not owned by a specific company (N3-a): "We talk about issues that are known in principle, which I can look up somewhere. This is not worth to be protected like a development aid. If I develop a new engine for example, that is something I have to keep to myself at first". We found that such open knowledge refers to knowledge that concerns all members of the network (N4-f): "Any situation where exchange is generated through mistakes, where a company has problems like with stipulation, or construction contracts, knowledge is exchanged because all have the same problems there". Interviewees reported that topics that concern all members are market-related, compliance-related, and legal issues. We found two motives why members switched to being open only to a certain topic.

Legal restrictions to share competitive knowledge: One reason why members only share market, compliance, or legal knowledge is that they are forced by law (N4-b): "the [representatives of the] organisations that were present in the meeting room signed a contract that they do not talk about business or project-related things". They are not allowed to discuss anything related to price rigging, for example. We found that the network management uses IT like electronic newsletters or email for distributing guidelines to enhance the awareness towards these restrictions (N4-b): "there are guidelines that we share before the meetings. This is a matter of the liability of an organisation how we handle this". Hence, networks utilise IT that is dedicated to communicate and distribute in a way that it restricts the sharing to a specific topic (N4-f): "they report about new guidelines, new norms. Maybe also about problems that occurred. This form of information, i.e., newsletters, […] is sent via email nowadays as a core product of [network]".

Collaborate with competitive members: Interviewees reported that the network management established meetings to share knowledge about the market and legal issues in which also competitors participate. Hence, members have to deal with the risk that competitive knowledge could spill over. To reduce that risk, the network management has the obligation to decide which type of knowledge should be distributed after standardisation and anonymisation of the content via collaborative IT (N4-a): "I take over and anonymise everything that lands on my desk, also requests. That's the essential thing. That is I will never say 'a firm has this and that problem'". We also found that construction sites are environments where competitive knowledge can spill over unintentionally. However, the need for collaborating on site drives network members to share only knowledge about certain topics: "we have our own concrete mixing plant. Of course, we would not share the recipes of certain concrete mixtures. […] We would share knowledge on how to build because we don't have secrets there […] the more transparent, the better for the site supervisors. Otherwise, if you build a road mysteriously, more and more questions come up". This shows that the problems of collaborating with competitors can be amplified by legal restrictions.

Interviewees reported that network homepages are only used for specific, non-competitive knowledge (N3-f): "There is a homepage of the network. There is a member section where tips and tricks on legal issues are provided […] how to write an adhortatory letter, these general things […] you'll find less domain-specific expertise there".

5 Discussion

We elicited three patterns in which network members switch from open to protective sharing behaviour. We described the patterns, highlighted the motives for open knowledge sharing in networks and for switching from sharing to protection and described examples of how members consequently adapt their use of collaborative IT. In the following, we discuss these patterns in the light of pertinent literature to explain our findings in terms of (a) the motives and practices for switching from open to protective, and (b) capabilities needed to manage the different switches, and how collaborative IT could enhance these capabilities. We elaborate on how members switch in different types of networks. Based on that, we discuss capabilities for these categories of networks necessary to foster the respective switching behaviour of members, and how the adapted use of collaborative IT could enhance these capabilities.

5.1 Switching behaviour and network types

All investigated networks were founded to foster knowledge sharing. However, we found that members switched from sharing to being protective in three ways: being open to (a) a certain extent (extent), (b) a certain group (group), and (c) a certain topic (topic). We found that sharing and protection should not be considered as stable states, i.e., members do not ex ante decide to share or protect, it is rather a phenomenon that is influenced by changes in the network itself, such as changes in the community, the network structure or network culture. These changes of the network trigger the switches from sharing to protection. Thus, we argue that considering network characteristics provides a more accurate understanding of sharing and protection phenomena.

Contrasting network categories with switching patterns, we identified that members from regionally unbounded networks rather reduce the details of their shared knowledge while members of regional networks rather restrict the sharing to specific groups or topics (see Table 3). The three types of switching behaviour are not mutually exclusive within a certain type of network, however, we found that being open to a certain extent mainly took place in regionally unbounded networks.

	Regionally unbounded	Regionally bounded
Homogeneous		N3 **(topic)**, N4 **(topic)**
Heterogeneous	N1 **(extent)**, N5 **(extent)**	N2 **(group)**, N6-10 **(group)**

Table 3. Geographical and professional proximity related to switching behaviour

Drawing on literature on proximities, this result is not surprising. Long distances between network members exacerbate the exchange of tacit knowledge (Schamp et al., 2004). Co-located members have better opportunities to hold face-to-face meetings to share tacit knowledge. Since tacit knowledge is more likely to be the source of competitive advantage (Norman, 2002), members are more restrictive and completely hide certain types of knowledge (topics). Being open to a certain group also fits well to pertinent literature. Geographical proximity correlates with social proximity as it is easier for people to meet in person and interact with each other (Handfield and Bechtel, 2002). In other words, the smaller the distance, the more likely is a high social proximity between members (Boschma, 2005). The easier adoption and use of knowledge with the same network configuration enhances the risk that local competitors apply leaked knowledge which explains why members only share with trusted subgroups of these co-located members. Hence, being open to a certain group seems especially prevalent in networks where members have high geographic proximity. We found that members in regionally bounded, homogeneous networks strongly focus on sharing knowledge about certain topics. We argue that this is because homogeneous members have a high professional proximity (cf. Schamp et al., 2004) which increases the risk of knowledge absorption. Especially when located in the same region, the risk of losing competitive knowledge to a direct competitor is high. Hence, members only share non-competitive knowledge.

Based on the proposition that the switching behaviour of network members depends on the network characteristics we will argue in the following that network members need to develop certain capabilities to switch towards being protective.

5.2 Protection capabilities to manage switching behaviour

We identified three patterns of switching behaviour with different requirements regarding knowledge protection. Hence, each organisation needs protection capabilities to manage the corresponding switch.

Competitiveness depends on the capabilities of network members to manage knowledge, here specifically on protection capabilities to balance sharing and protection of knowledge. Capabilities involve complex patterns of various resources and people, and are made up of a sequence of organisational routines (Grant, 1991). Various types of protection capabilities have been proposed, such as formal and strategic (e.g., De Faria and Sofka, 2009) or organisational (Liebeskind, 1996). The various types of capabilities can be aggregated to concealment, ambiguity, and enforcement capabilities (Manhart, 2015). Concealment describes the capability to reduce the risk that a competitor identifies knowledge. Ambiguity describes the capability to reduce the risk that a competitor assimilates knowledge or imitates core competencies. Enforcement describes the capability to reduce the risk that a competitor uses the assimilated knowledge or imitated core competence in form of business strategies.

Concealment: Reducing the risk of identification refers to the reduction of knowledge observability. This depends on two characteristics: the extent of disclosure (Winter, 1987), as well as the ease of understanding and examining different parts of knowledge (Zander, 1991). In other words, the success of externals to identify knowledge of a focal firm depends on the level of disclosure and whether the knowledge can easily be recognised as valuable.

We suggest that being open to a certain topic is a switching pattern that requires the capability of concealment. That is because members need to hide certain types of knowledge completely. As an example, we found that hiding competencies is practiced to avoid headhunting (N8-f): “if we employ a person that has unique skills, we hide this person from the company homepage so that others cannot identify his skills”. We also found that competitive members organise workshops to be up to date on new standards and norms or market news while they protect how they build products (N4-b): “in the meeting room […] they do not talk about business or project-related things but […] about market-relevant things” and (N4-f): “they report about new guidelines, new norms”. Since we observed that especially members of regionally bounded networks with high professional homogeneity perform this switching pattern, concealment capabilities seem of particular interest for them. As a starting point to build concealment capabilities, organisations need to be able to control the extent of disclosure and the ease of understanding by externals. Here, the basis to build routines is a proper classification of knowledge documents (Desouza and Vanapalli, 2005) and the traceability of knowledge development in activity streams (Pawlowski et al., 2014). This helps members to distinguish the types of knowledge within their organisation. This way, organisations build the ground for classifying knowledge according to its criticality and maintain integrity by tracing who accessed and developed the documents. Such documents can be managed by collaborative IT for which members can implement role-based access control (Bertino et al., 2006). Thus, organisations can ensure that only certain types of knowledge are identified and accessed by certain people. Such a technical implementation could support members to manage the process of switching and could build the basis for developing routines to conceal knowledge types from other network members.

Ambiguity: It takes more to assimilate new knowledge than just exposing individuals to it (Pennings and Harianto, 1992). One way of reducing the risk of unwanted assimilation by other members is to establish and maintain causal ambiguity. Causal ambiguity describes the nature of causal relationships between actions and results (Lippman and Rumelt, 1982) and helps to build barriers to imitation (Reed and Defillippi, 1990). In other words, members need to disguise from competitors how they combine knowledge to build competencies. A competitor should not be able to see how different parts of the knowledge relate to a product or competency.

We suggest that being open to a certain extent is a switching behaviour that requires the capability of ambiguity. That is because members reveal their knowledge on a very high level but disguise detailed knowledge. They protect details of their knowledge that are needed to build competencies to develop a product. As an example, interviewees reported that they do not reveal detailed knowledge about the sensor technology in their products (N8-f): “There are limits […] we work with opto-sensors, [if people want to know] what sensors we have in our products, we draw the line there”. This way, other members can observe the knowledge but are not able to understand how different aspects relate to each other so that they understand causal relationships of knowledge. As we observed that particularly members of regionally unbounded networks with low professional proximities perform this switch, ambiguity capabilities to disguise their competencies seem of particular interest for them.

As a starting point to build ambiguity capabilities, organisations need to be able to determine different levels of detail for their knowledge. Based on that, they need to be able to increase the causal ambiguity for competitors. This could be done by separating between different versions of documents, i.e. a copy intended for externals where the relationship between knowledge components can hardly be detected. As an example, members make their software programs more complex before sharing them with competitors (N3-e): “We protect the programs that we write by handing over ‘wrong’ program copies […]. This is something we like to do, to make programs so complicated that nobody can read them anymore […] you are not able to make use of it, because the effort is too high to bring everything together”. The different versions of knowledge with different levels of detail, then could be managed via role-based access control (Bertino et al., 2006). Interviewees explained that they form groups to cope with reluctant members and create group appearances on forums. Based on our findings, the complementary use of collaborative IT could help in this regard. Providing IT like a group workspace in a forum could enhance members’ ambiguity capability by providing coordination space to determine the detail of knowledge to be shared.

Enforcement: Once competitors assimilated knowledge and are able to put it into practice, i.e. build a business strategy that exploits the assimilated knowledge best by assuring appropriability of returns (Maier, 2007, Grant, 1991), members need to enforce protection. There are two main ways to protect knowledge after being disclosed and assimilated. Protection (1) via IPR (Hertzfeld et al., 2006, Liebeskind, 1996) and (2) building trust to prevent externals from opportunistic behaviour (Norman, 2002). We found that members switch to being open to a certain group for these two reasons.

We suggest that being open to a specific group is a switching behaviour that requires the capability of enforcement. That is because members establish trust by forming subgroups where they can openly share. As an example, interviewees reported that they try to combine both legal protection and trusted relationships: they found working groups where they want to openly share and drive innovations since they enable to get to know each member in the group better but at the same time sign a letter of intent and NDA to assure that openly sharing has no serious consequences (N7-e): “A working group is founded but still on a level that not all share in a way that it is useful for the group […]. If there is an NDA or a letter of intent of such a group, this would enable to go this way more serious”. As we observed that especially members of regionally bounded networks with low professional proximities perform this switching pattern, enforcement capabilities seem of particular interest for them. We argue that the definition of confidentiality levels for knowledge linked to groups is crucial to build enforcement capabilities. Based on that, IT could help to overcome the challenge to manage the submission and approval of NDAs (Prajapati et al., 2013) with various stakeholders or the violations of IPR. Based on our findings, the complementary use of collaborative IT could support members to address this challenge. As an example, network management could provide an IPR management tool (e.g., Bellini et al., 2013) that focuses on increasing transparency in the dissemination process and requires commitment from all members of the group. This way, organisations could circumvent the problem of enforcing legal measures and simultaneously increase the trust between members due to increased transparency.

The following table depicts the identified patterns of switching behaviour, triggers of the switch, collaborative IT used, and the protection capabilities needed to manage the switch.

	Open to certain extent	Open to certain group	Open to certain topic
Description	Share general knowledge & protect details	Share with subgroups of the network	Share knowledge only about a certain topic
Trigger	• Reluctance to contribute • Fear of imitation • Fear of recourse	• Problems to enforce legal measures • Uncertainty about sharing behaviour	• Legal restrictions to share about topic • Collaboration with competitors
Collaborative IT	Use forums/ blogs for high level sharing and synchronous communication for detailed sharing	IPR tool to enforce NDAs: collaboratively agree on dissemination	Use of collaborative IT to increase awareness towards knowledge protection
Protection capability	Ambiguity	Enforcement	Concealment

Table 4. Description of the three Switching Patterns

We also see several shortcomings and limitations of our study. First and in line with exploratory case study designs, we do not claim generalisability of our findings, as we do not use a representative sample. We do not claim completeness of our switching patterns, e.g., network members might switch back from being protective to being more open. We did not explicitly focus on such phenomena and we only found evidence for switching from openly sharing to being more protective and not vice versa. Another limitation is that we conducted the interviews in German and translated them into English. We minimised the translation bias as the researchers double-checked the translations. Regarding the selection of informants by key informants, we argue for our approach as the key informants seemed to have the best knowledge for purposefully selecting informants in their networks (Abdolmohammadi and Shanteau, 1992).

6 Conclusion

In this paper, we investigated the relationship between sharing and protection behaviour in SME networks, more specifically, the motives and practices of members switching from sharing to protection. We identified three patterns of switching behaviour: members switch from sharing to being open to a certain (a) extent, (b) group, or (c) topic. We found that changes in the networks and network characteristics are associated with the switches. Our findings demonstrate that organisations should not consider sharing and protecting as stable states, i.e., members do not ex ante decide to share or protect. Rather, sharing and protection behaviour is related with network characteristics and changes in the network. Hence, we argue that considering sharing and protection in connection with network characteristics and changes in communities, network structure, or culture, provides a more accurate understanding of sharing and protection phenomena. We found that members of SME networks adapt the use of collaborative IT to manage the switches from sharing to protection. This demonstrates that collaborative IT is not always in conflict with protection behaviour but can complement it through adapted use. Collaborative IT should also provide services, which can be used for knowledge protection according to the needs expressed by our interviewees. If users are more confident that they can effectively protect their crucial knowledge, they might also be more willing to share.

Our findings have several implications for practitioners organised in such networks. First, members need protection capabilities to manage the switches. More specifically, the three switching patterns seem to be associated with particular protection capabilities. Network members especially need ambiguity capabilities to manage switch (a) being open to a certain extent, enforcement capabilities to manage switch (b) being open to a certain group and concealment capabilities to manage switch (c) being open to a certain topic. We gave examples how collaborative IT could enhance these protection capabilities. Concerning the scientific implications of our study, our switching patterns contribute a new perspective for furthering the understanding of knowledge protection. First, balancing sharing and protection is not static, but dynamic. Second, research on the design of IT artefacts might consider that collaborative IT can be also designed to allow users to switch towards being more protective.

Future research should also investigate regionally unbounded, homogenous networks it might also be of value to explore reverse switching patterns from being protective to being open. Scholars should further investigate the enhancement of protection capabilities through the adapted use of collaborative IT. Future work could look at how network management can support this enhancement by providing infrastructure or services for collaborative IT. Another direction for future research could be to investigate the switching phenomena over time. How does switching behaviour change in relation to the maturity of networks? How do network dynamics like the merger of networks or the expansion of networks affect the knowledge protection behaviour of their members? These questions could be of interest to better understand knowledge protection in networks as well as help design a network infrastructure that fosters protection capabilities to help members balance sharing and protection.

Acknowledgments:

This work was co-funded by the European Commission under the 7th Framework Programme (FP7), Integrating Project LEARNING LAYERS (project no. 318209).

References

Abdolmohammadi, M. J. and Shanteau, J. (1992)."Personal Attributes Of Expert Auditors", *Organizational Behavior and Human Decision Processes*, 53 (2), 158-172.

Ahmad, A., Bosua, R. and Scheepers, R. (2014)."Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective.", *Computers & Security,* 42 (May), 27-39.

Andersén, J. (2012)."Protective capacity and absorptive capacity: Managing the balance between retention and creation of knowledge-based resources", *The Learning Organization*, 19 (5), 440-452.

Argote, L. and Ingram, P. (2000)."Knowledge Transfer: A Basis For Competitive Advantage In Firms", *Organizational Behavior and Human Decision Processes*, 82 (1), 150-169.

Arundel, A. (2001)."The relative effectiveness of patents and secrecy for appropriation", *Research policy*, 30 (4), 611-624.

Baughn, C. C., Denekamp, J. G., Stevens, J. H. and Osborn, R. N. (1997)."Protecting Intellectual Capital In International Alliances", *Journal of World Business*, 32 (2), 103-117.

Bellini, P., Bruno, I., Nesi, P. and Paolucci, M. (2013). "Institutional Services And Tools For Content, Metadata And Ipr Management", pp. 20-25.

Bertino, E., Khan, L. R. and Sandhu, R. (2006)."Secure Knowledge Management: Confidentiality, Trust, And Privacy", *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans,* 36 (3), 429-438.

Boschma, R. (2005)."Proximity And Innovation: A Critical Assessment", *Regional Studies,* 39 (1), 61-74.

Bou-Llusar, J. C. and Segarra-Cipre´S, M. (2006)."Strategic Knowledge Transfer And Its Implications For Competitive Advantage: An Integrative Conceptual Framework", *Journal of Knowledge Management,* 10 (4), 100 -112.

De Faria, P. and Sofka, W. (2009). "Knowledge Protection Capabilities And Their Effects On Knowledge Creation And Exploitation In High-And Low-Tech Environments", *Advancing the Study of Innovation and Globalization in Organisations (ASIGO) Conference*, Nuremberg, Germany.

De Faria, P. and Sofka, W. (2010)."Knowledge Protection Strategies Of Multinational Firms-A Cross-Country Comparison.", *Research Policy,* 39 (7), 956-968.

Desouza, K. C. and Vanapalli, G. K. (2005)."Securing Knowledge In Organisations: Lessons From The Defense And Intelligence Sectors", *International Journal of Information Management,* 25 (1), 85-98.

Easterby-Smith, M., Lyles, M. A. and Tsang, E. W. (2008)."Inter-Organizational Knowledge Transfer: Current Themes And Future Prospects", *Journal of Management Studies,* 45 (4), 677-690.

Grant, R. M. (1991). "The Resource-Based Theory Of Competitive Advantage: Implications For Strategy Formulation", in Zack, M. H. (Ed.) *Knowledge and Strategy*, BUtterworth-Heinemann, Woburn, pp. 3-23.

Handfield, R. B. and Bechtel, C. (2002)."The Role Of Trust And Relationship Structure In Improving Supply Chain Responsiveness", *Industrial Marketing Management,* 31 (4), 367-382.

Hertzfeld, H. R., Link, A. N. and Vonortas, N. S. (2006)."Intellectual Property Protection Mechanisms In Research Partnerships", *Research Policy,* 35 (6), 825-838.

Jennex, M. and Durcikova, A. (2013). "Assessing Knowledge Loss Risk", in *2013 46th Hawaii International Conference on System Sciences (HICSS),* Wailea, HI, USA, pp. 3478 - 3487.

Jennex, M. and Durcikova, A. (2014)."Integrating IS Security with Knowledge Management: Are We Doing Enough?", *International Journal of Knowledge Management* 10 (2), 1-12.

Jennex, M. E. and Zyngier, S. (2007)."Security As A Contributor To Knowledge Management Success", *Information Systems Frontiers,* 9 (5), 493-504.

Kale, P., Singh, H. and Perlmutter, H. (2000)."Learning And Protection Of Proprietary Assets In Strategic Alliances: Building Relational Capital", *Strategic Management Journal,* 21 (3), 217-237.

Lee, S. C., Chang, S. N., Liu, C. Y. and Yang, J. (2007)."The Effect Of Knowledge Protection, Knowledge Ambiguity, And Relational Capital On Alliance Performance", *Knowledge and Process Management,* 14 (1), 58-69.

Leiponen, A. and Byma, J. (2009)."If You Cannot Block, You Better Run: Small Firms, Cooperative Innovation, And Appropriation Strategies.", *Research Policy,* 38 (9), 1478-1488.

Lertpittayapoom, N., Paul, S. and Mykytyn, P. (2007). "A Theoretical Perspective On Effective Interorganizational Knowledge", in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on,* p. 187b.

Liebeskind, J. P. (1996)."Knowledge, Strategy And The Theory Of The Firm", *Strategic Management Journal,* 17 (Winter Special Issue), 93-107.

Lin, C., Wu, Y. J., Chang, C., Wang, W. and Lee, C. Y. (2012)."The Alliance Innovation Performance Of R&D Alliances-The Absorptive Capacity Perspective.", *Technovation,* 32 (5), 282-292.

Lippman, S. A. and Rumelt, R. P. (1982)."Uncertain Imitability: An Analysis Of Interfirm Differences In Efficiency Under Competition", *The Bell Journal of Economics,* 13 (2), 418-438.

Maier, R. (2007). *Knowledge Management Systems: Information And Communication Technologies For Knowledge Management*, Springer, Berlin.

Malhotra, A., Gosain, S. and Sawy, O. A. E. (2005)."Absorptive Capacity Configurations In Supply Chains: Gearing For Partner-Enabled Market Knowledge Creation.", *MIS Quarterly,* 29 (1), 145-187.

Manhart, M. (2015). "A Capability Model for Knowledge Protection", in *Proceedings of the 12th International Conference on Wirtschaftsinformatik (WI2015),* Osnabrück, pp. 572-584.

Manhart, M. and Thalmann, S. (2015)."Protecting Organizational Knowledge: A Structured Literature Review.", *to appear in Journal of Knowledge Management,* 19 (2).

Mayring, P. (2014). "Qualitative Content Analysis", *Theoretical Foundation, Basic Procedures and Software Solution*, Klagenfurt, Austria, Beltz.

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

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), 81-88.

Pennings, J. M. and Harianto, F. (1992)."The Diffusion Of Technological Innovation In The Commercial Banking Industry", *Strategic Management Journal,* 13 (1), 29-46.

Prajapati, V., Tripathy, S. and Dureja, H. (2013)."Product Lifecycle Management Through Patents And Regulatory Strategies", *Journal of Medical Marketing: Device, Diagnostic and Pharmaceutical Marketing,* 13 (3), 171-180.

Reagans, R. and Mcevily, B. (2003)."Network Structure And Knowledge Transfer: The Effects Of Cohesion And Range", *Administrative Science Quarterly,* 48 (2), 240-267.

Reed, R. and Defillippi, R. J. (1990)."Causal Ambiguity, Barriers To Imitation, And Sustainable Competitive Advantage", *The Academy of Management Review,* 15 (1), 88-102.

Roberts, J. (2000)."From Know-How To Show-How? Questioning The Role Of Information And Communication Technologies In Knowledge Transfer", *Technology Analysis & Strategic Management,* 12 (4), 429-443.

Schamp, E. W., Rentmeister, B. and Lo, V. (2004)."Dimensions Of Proximity In Knowledge-Based Networks: The Cases Of Investment Banking And Automobile Design", *European Planning Studies,* 12 (5), 607-624.

Thalmann, S. and Manhart, M. (2013). "Enforcing Organisational Knowledge Protection: An Investigation of Currently Applied Measures", in *pre-ICIS workshop on Information Security and Privacy (SIGSEC),* Milan, Italy.

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), 28-42.

Trkman, P. and Desouza, K. C. (2012)."Knowledge Risks In Organizational Networks: An Exploratory Framework", *Journal of Strategic Information Systems,* 21 (1), 1-17.

Tsai, W. (2001)."Knowledge Transfer In Intraorganizational Networks: Effects Of Network Position And Absorptive Capacity On Business Unit Innovation And Performance", *Academy of management journal,* 44 (5), 996-1004.

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

Wagner, S. M. and Bukó, C. (2005)."An Empirical Investigation Of Knowledge-Sharing In Networks", *Journal of Supply Chain Management,* 41 (4), 17-31.

Winter, S. G. (1987). "Knowledge And Competence As Strategic Assets", in Teece, D. J. (Ed.) *The Competitive Challenge: Strategies for Industrial Innovation and Renewal*, Ballinger, Cambridge, MA, pp. 159-184.

Zander, U. (1991). "Exploiting A Technical Edge: Voluntary And Involuntary Dissemination Of Technology", *Stockholm: Institute of International Business (IIB), Stockholm School of Economics*, p. 253.