4.2 Collaborating in a Research and Development Project: Knowledge Protection Practices applied in a Co-opetitive Setting

Rene Kaiser[31], Stefan Thalmann[32], Viktoria Pammer-Schindler[33] and Angela Fessl[34]

Abstract: Organisations participate in collaborative projects that include competitors for a number of strategic reasons, even whilst knowing that this requires them to consider both knowledge sharing and knowledge protection throughout collaboration. In this paper, we investigated which knowledge protection practices representatives of organizations employ in a collaborative research and innovation project that can be characterized as a co-opetitive setting. We conducted a series of 30 interviews and report the following seven practices in structured form: restrictive partner selection in operative project tasks, communication through a gatekeeper, to limit access to a central platform, to hide details of machine data dumps, to have data not leave a factory for analysis, a generic model enabling to hide usage parameters, and to apply legal measures. When connecting each practice to a priori literature, we find three practices focussing on collaborative data analytics tasks had not yet been covered so far.

Keywords: Knowledge Sharing; Knowledge Protection; Protection Practices; Collaboration;

1 Introduction

Current trends such as globalisation and digitization demand inter-organisational knowledge sharing [ITM18]. Organizations increasingly need to absorb external knowledge in order to remain competitive [LA08]. Knowledge sharing networks are collaboration structures that allow organisations not only to acquire and share knowledge, but also to collaboratively develop knowledge [TS18]. Via such networks, organizations become part of an environment in which knowledge is distributed over its member organizations and in turn over the people working in the member organizations [SCK11].

In such networks, organizations benefit from joint knowledge sharing and creation with external partners, but also have the risk to lose competitive knowledge to partners (especially to competitors) also engaging in the same networks [TI18]. Thus, in addition to knowledge sharing and creation activities, organisations also need to protect own critical

[31] Know-Center – Research Center for Data-Driven Business & Big Data Analytics, Graz, Austria
[32] University of Graz and Institute for Interactive Systems and Data Science, Graz University of Technology
[33] Know-Center and Institute for Interactive Systems and Data Science, Graz University of Technology
[34] Know-Center – Research Center for Data-Driven Business & Big Data Analytics, Graz, Austria

knowledge [JM16]. As a consequence, balancing knowledge sharing and protection is a major challenge for participants in inter-organizational knowledge sharing networks [LFP16].

In this paper we present a study in the setting of a collaborative European research and innovation project with 37 partner organisations as an instantiation of a knowledge sharing network. We have carried out 30 interviews on knowledge sharing and protection practices. We describe overall seven salient knowledge protection practices, and discuss them in a structured way.

The main contribution of our work is threefold: fist, we could confirm that there is a need for knowledge-intensive companies to participate in knowledge sharing networks. Secondly, we therefore suggest to refer to such co-opetitive collaboration structures as "knowledge sharing and protection networks". Thirdly, we elaborate on seven knowledge protection practices and relate them to prior literature.

2 Background and Related Work

Knowledge creation theory views an organization as a knowledge-creating entity, arguing that not only knowledge but also the capability to create, share, and utilize knowledge are the most important sources of a firm's competitive advantage [Non94]. Knowledge creation in organizations has been regarded as 'knowledge conversion', which spans individual, group, and organizational levels [Non94]. Knowledge creation in inter-organizational contexts demands the additional capability of protecting knowledge [TD12] and when it simultaneously involves cooperation and competition (i.e. shared knowledge may be used for competition), it is called *co-opetition* [LLP03]. Organizations therefore have to manage *knowledge sharing* under co-opetition and thus balance knowledge sharing and protection [LFP16] [MT15].

Despite knowledge protection being a core strategy of knowledge management [BS01], it is mainly investigated on a conceptual level for explicit knowledge in formal settings [MT15]. According to [MTM15], knowledge protection can (1) focus on restricting the sharing within a certain communication channel, i.e. participate in a knowledge sharing network, (2) focus on restricting the sharing with specific sharing partners, i.e. share only with trusted peers or (3) focus on restricting the sharing of concrete knowledge artefacts, i.e. knowledge related to a certain topic.

Literature largely views knowledge protection as a coordinative and contractual task in dyadic relationships, such as joint ventures or the cooperation of large international enterprises, but neglects complex relationships, such as in networks [HST15] [PMW15]. Data-centric collaborations in co-opetitive settings are not investigated from a knowledge protection point of view so far. To tackle this research gap and to shed more light on the challenge of balancing knowledge sharing and protection in data-centric co-opetitive settings, more research is required to understand which concrete protection practices and measures can be applied.

3 Methodology

3.1 Context: Co-opetitive Collaborative Research and Innovation Project

This paper investigates the setting of a cross-organisational European research project. 37 institutions from five European countries collaborate in this project. Of these, 16 are research institutions and several of the involved companies are active in the same market, and hence in competition to each other. More than 600 people are actively involved in the project. The project addresses challenges for innovating in semiconductor and electronics manufacturing, focusing on topics such as data analytics and production process optimization. The power semiconductor and electronics manufacturing field is a high-tech industry and a very knowledge-intensive sector; meaning that core technological knowledge is for every company a key asset. Any details about products and their manufacturing are confidential by default. This encompasses for example production and process know-how, insights into physical and chemical processes, knowledge about technical approaches and advanced technologies, or data encapsulating implicit details regarding procedures, practices, machines and even customers. It is essential for industry partners to avoid any risks of knowledge spill-over or indirect leakage towards competitors via third parties. Risk mitigation and knowledge protection are very serious concerns as they don't want to jeopardise their competitive advantages and market position.

Collaboration within the setting of a cross-organisational European research project makes sense for member organisations as the key questions of the project do not target core competitive knowledge (yet); and the European Commission provides funding for this collaboration that would not be available without the networked project setting. However, member organisations, represented by individual project members, are also concerned that collaboration within the project may still inadvertently give competitors insights into critical knowledge and procedures.

The project can therefore be understood as a setting of a co-opetitive endeavour, a setting in which member organisations follow the strategy to combine competition and cooperation with each other [GJ11] [Lu07].

3.2 Study Design

We conducted semi-structured interviews using an interview guideline focussing on how the interviewee is involved in the collaboration and communication with project partners, as well as how they deal with the tension of sharing and protecting sensitive knowledge in collaboration. We also asked which tools and infrastructures are used, and how benefits and risks of knowledge sharing are assessed.

We conducted 30 interviews, 28 of them via a remote audio connection (telephone or Skype) and two of them face-to-face. We argue that with this number of interviews we cover the breadth of the project sufficiently, and as an indicator towards that we saw saturation with respect to new insights in this sample. To invite interviewees, we applied

a purposeful sampling, i.e. we focussed on project members who are actively involved in the cross-organisational collaboration. With consent of the interviewees, the interviews were recorded for subsequent analysis. To refer to the interviews in anonymized form they are coded with IDs *IN01* to *IN30*. Interviews were conducted in English or in German. Any quotes in German have been translated to English. Quotes have been anonymized to hide the names of persons and institutions as well as to protect the identity of the interviewees themselves.

For a concise overview, the descriptive statistics of our sample are depicted in Table 1.

Number of interviews	30
Interviewees (female/male)	31 (5/26)
Work experience	AVG 15.75 years
Interview duration	20 – 70 min, AVG ~40 min
Interview language	German: 25; English: 5
Interviewee country	AT: 13; DE: 12; IT: 2; PT: 3

Table 1: Details about the interview sample. One interview involved two interviewees.

The recordings of the interviews have been transcribed. Then, the analysis process followed the qualitative content analysis according to Mayring [Ma14]. The first step of analysis towards understanding the project partners' knowledge protection behaviour was to process all answers that are directly relevant for this topic. All relevant statements were filtered out and this subset was further analysed by assigning codes. Codes emerged via *inductive* category development. After this iterative coding process, three main code categories emerged that group the statements along three distinct aspects: (1) #*protectionConcern*: statements describing the knowledge which is to be protected as well as the rationale to protect it, (2) #*aspectOfBalancing*: statements discussing the process of deciding on a protection practice and the factors of the decision, and (3) #*protectionMeasure:* statements mentioning concrete measures for protection. The category (3) emerged out of 27 more specific sub-codes which it aggregates, each of the 27 corresponding to a knowledge protection measure – to name one example: to share results but never share details about the underlying process which is subject to intellectual property. See Table 2 for an overview and the Appendix for a detailed visualisation.

Category name	**(1) #protectionConcern**	**(2) #aspectOfBalancing**	**(3) #protectionMeasure**
Description	Knowledge that should be protected as well as reasons for protection.	Decision on how the balancing of sharing and protecting is handled.	Concrete measures that have been mentioned.
Number of statements	79	138	115

Table 2: Three categories have emerged based on a coding process, structuring all answer statements.

During our analysis we found typical logical sequences for the three aforementioned categories. We clustered these sequences into seven knowledge protection practices, which we present in the subsequent results section. Each practice condenses evidence from multiple interviews, and interviewees employ multiple practices in different situations.

4 Results: Knowledge Protection Practices

Below we describe in structured form the seven practices identified in our study:

4.1 Practice 1: Restrictive Partner Selection

Project members protect their interests by carefully choosing at setup time whom to collaborate with in a close manner, or at all. Competitive partners might join the same project consortium, but not directly collaborate in the structures of the project where the actual work is performed. *IN19* represents a company partner and explains:

> "*Of course I pay attention to intellectual property. At project setup time I make sure that the tasks are structured in modular and encapsulated fashion, and I very carefully select the partners who work with me in a certain task. When this is cleanly set up, and only those who really contribute join, rather than those who just wish to join as well, then the IP issues in daily project business are mitigated.*"

WHY – The rationale behind not directly collaborating with all partner organisations is to avoid risks of revealing sensitive knowledge to these partners. Applying this practice spares the continuous decision-making efforts to balance sharing and protecting knowledge when collaborating.

WHAT – Subject to protection is any sensitive partner knowledge that may become visible or is generated in the collaborative project.

CONSTRAINTS – Since partnerships with partners in a consortium can be of strategic interest, a compromise to forfeit this practice may be taken in favour of other interests.

IMPLICATIONS – By avoiding collaborations with risky partners like competitors, knowledge spill-over risks can be minimized and any communication involving potentially sensitive knowledge becomes more straightforward. However, avoiding to closely communicate with certain partners also impedes any impact and innovation stemming from such collaborations.

DECISION PROCESS/FACTORS – Partners weighing the risks, as well as the pros and cons of collaborating with a certain partner on a certain topic. They might also consider not to collaborate with further partners who have close ties to their competitors.

4.2 Practice 2: Communication through Gatekeeper

Defining a rule that all communication should be authorized by the designated gatekeeper. Frequently, this is made transparent to partners. *IN01* reflects on this role:

> „*I strive to check the project's file share once a week to see if there is something that is relevant for us, and forward it internally, but this means I am something like the internal information gatekeeper. So I have to check everything and distribute internally. (...) And that requires effort of course. (...) Naturally among the colleagues in the project this creates an information imbalance.*"

WHY – A project partner might strive for full control over all knowledge exchanged and consider it safer to have it all handled by a single responsible person capable of balancing the sharing and protection decisions in their best interest.

WHAT – Subject of protection are any contents of the project and any sensitive knowledge belonging to the partner applying this protection practice.

CONSTRAINTS – The larger the project team, the closer the direct collaboration, and the more people are directly in contact, the more difficult it becomes to manage this role.

IMPLICATIONS – A gatekeeper can be very efficient in deciding from case to case what to share or not, but gatekeepers can also be a bottleneck and difficult to replace.

DECISION PROCESS/FACTORS – This practice is only applicable, if the complexity and nature of the direct collaboration with partners can be handled by such a role.

4.3 Practice 3: Limit Access to Central Platform to a Small Number of People

Only a small number of people per organisation get access to the sharing platform, and the rule is to only use this platform for classified knowledge.

WHY – The risk of knowledge leakage is considered lower when only few partner representatives have accounts and thus access.

WHAT – Documented knowledge and data stored in IT systems.

CONSTRAINTS – Sharing partners need to be willing to use this platform and accept the overhead and bottleneck issues inherent to this knowledge protection practice.

IMPLICATIONS – This practice can help to protect sensitive knowledge by restricting access to few persons, hence reducing risks of illegal access and sharing. However, this practice can be a critical bottleneck causing communication overhead and delays.

DECISION PROCESS/FACTORS – The improved protection comes with higher overhead and coordination. *IN25* acknowledges this trade-off:

> *"The only thing would be access to (this platform), which could be made easier or allowed for more people, this is the only constraint but I also regard it as necessary.*"

4.4 Practice 4: Hide Details of Machine Data Dumps

The owner of the data makes sure any sensitive details are removed from the data set before it is shared. What also needs to be taken into account is the purpose of it being processed by the external partner: hiding or obfuscating too much may imply the data is not suitable for further processing anymore. *IN11* stated:

> "*I think we would pass on simulated or anonymized data if that were the case, (...) that you, very concretely, simply replace the machine names for example with M1 to M200 or so, such that it is no longer traceable which machines are actually in the factory. But such that still the data flow can be understood, in the way that you can say this was handled by this machine and then it went there. That way you can draw conclusions, but it is a sufficient granularity for the project.*"

From the perspective of the partner receiving the data set, *IN21* acknowledges that anonymized data can be sufficient:

> *"(...) get excerpts of data which are anonymized which essentially is enough for us. If a product is named A or X, Y, Z is not relevant for the information we provide."*

WHY – Partners sharing data sets need to make sure the data shared does not contain any confidential knowledge.

WHAT – Any confidential details contained explicitly, or any implicit knowledge which could be made visible via advanced analysis or aggregation with further data sets.

CONSTRAINTS – It might turn out that no solution can be found that balances both the protection needs and the (level of) details required for the collaboration.

IMPLICATIONS – Data sets can be shared with external partners who may process them independently. But it is typically not clear what an expert can extract out of the data, hence there is still an undefinable inherent risk.

DECISION PROCESS/FACTORS – The sharing partner needs to carefully consider what sensitive knowledge is contained in the data set, at the same time making sure it is still useful with respect to the intended purpose.

4.5 Practice 5: Data Won't Leave Factory for Analysis

In contrast to transferring the data from the data owner to the analytics expert, the practice is to conduct the analytics via a secure remote connection and hence make sure the data remains within the industry partner's premises. *IN21* explains the setup in their use case:

> "*Yes, this is a topic for us indeed, since with our monitoring systems we have to analyse data to calculate KPIs etc. which stem from deep inside the production and are of course relevant for protection causes. (…) "Some of the data must not leave the factory. So we just analyse them on site, also we receive data excerpts which are anonymized. Which essentially is sufficient for us.*"

WHY – Industry partners tackle an advanced data analytics problem with collaborators and do not want the data to be processed outside their premises.

WHAT – The subject of protection is sensitive data stemming from e.g. production processes within an industry company.

CONSTRAINTS – Applying this measure may not be well suited when very interactive analysis is required where not having direct access to the data impedes progress. In any case, partners need to agree on an infrastructure to enable remote analysis, for example using Apache Zeppelin (https://zeppelin.apache.org/) and consider any risks of collaborating via a remote connection.

IMPLICATIONS – Data can be processed without leaving the factory, thus mitigating risks of knowledge spill-over, but not having direct access to the data may cause the analytics work to be inefficient.

DECISION PROCESS/FACTORS – Weigh the risk reduction against the additional communication effort and potential security risks of the remote connection itself.

4.6 Practice 6: Generic Model Hiding Usage Parameters

The idea behind this protection practice is to instead of fitting a model to the intended parameters, to instead develop a generic model that not only suits the eventual usage parameters but also the parameter space around them, e.g. by employing a Design of Experiments (DoE) [Mo09] modelling approach. This enables the user of the model to collaborate while not sharing these parameters.

WHY – The partner executing the model does not want the developer of the model to know which exact parameters they use. *IN27* as the developer of the model describes the challenge:

> "*With (user partner), there is some issue. (...) They use this (machine). And the (parameterization) is what they are very keen on. They don't want to disclose this. So the issue is, how can I model the (machine), can describe a process, if I don't know (machine details). (...) That's gonna be a kind of a challenge.*"

WHAT – The subject of protection is very sensitive process know-how.

CONSTRAINTS – This very specific knowledge protection practice is only applicable in certain constellations where the user of a model seeks to protect usage parameters, and developing a generic model is even possible.

IMPLICATIONS – With this protection practice, the process parameters can indeed be hidden as long as the possible parameter space is large enough to prevent determination. However, generic models require extra effort and handling requires extra communication overhead among partners. Further, generic models might also perform worse.

DECISION PROCESS/FACTORS – Investigate if the modelling can actually be done in a generic fashion, if the parameter space is complex enough to effectively hide the real set of parameters, if the generic model's quality is good enough for its intended use.

4.7 Practice 7: Apply Legal Measures

Beyond basic laws, partners apply legal measures to specify how their knowledge or intellectual property may be shared or exploited. Concrete measures are for example project consortium agreements, non-disclosure agreements (NDAs), or patents.

WHY – Contractual agreements among project consortia or individual partners typically form a legal framework based on which partners have a certain level of trust that whatever they share, invent or develop, it will only be used by their partners with their agreement.

WHAT – Subject of protection are any contents and outcomes of the joint project, as well as any prior knowledge of the partners or insights into their organisation.

CONSTRAINTS – Legal measures require a certain level of knowledge maturity and it is sometimes difficult to enforce the legal measures.

IMPLICATIONS – Legal agreements may provide the basis for a relatively open and fruitful collaboration, but they are sometimes costly to enforce or not very effective for immature knowledge.

DECISION PROCESS/FACTORS – Legal measures are a standard procedure but not very effective for immature and critical knowledge.

5 Discussion of Results

> "*There is no way to guarantee how the information will be used. Again, when we trust the other partners, we can be more confident. But at the end it is a human decision to share it or not.*" (IN20)

In our interviews we found seven practices which are applied to balance knowledge sharing and protection in our setting – a collaborative research and developing project in which among others, competitors are collaborating focussing on data-driven innovations in the semiconductor industry. We intend to contribute to the literature in two ways: (1) research on balancing knowledge sharing and protection focusses very much on dyadic relationships and research on more complex and interwoven collaboration structures is scarce [PMW15] [LFP16] [HST15]. In our case we investigated a complex knowledge sharing network which formed a project to acquire public funding and which can be characterized as co-opetition setting. (2) Research on knowledge sharing and protection mostly neglects the IT perspective so far [MT15] [ITM18]. We investigated an IT-mediated and data-centric collaboration and thus aimed at filling this gap.

In the practice **restrictive partner selection,** the communication partner selects less risky partners for collaboration and avoids collaborations with more risky partners. In the literature it is mentioned that the willingness to share can be limited to certain groups due to protection concerns [Ri15]. In this case, the formation of subgroups is mentioned as recommended practice [MTM15].

The **communication through a gatekeeper** channelizes the knowledge sharing through one person. This provides a lot of control to the company but can also be a serious barrier to knowledge sharing. In literature such strategy is also mentioned as persistent participation to control knowledge risks in which a less knowledgeable person takes the role of the gatekeeper and is not able to share the risky knowledge [JV16].

The **limitation of access to certain people** is well known from the information security literature and can be used to manage knowledge risks by defining role-based access models [TM13] [Th14]. Further, literature also reports about limiting the access to corporate social media accounts to avoid knowledge loss [STM15].

Hiding details of machine data dumps means to change the data shared with the partners. We found no technical procedure related to data and knowledge protection in the literature. But in general, the strategy of hiding details is mentioned frequently [MTM15] [MT15].

The practice to **not have data leave a factory for analysis** focusses on a collaborative data science project and is specific for a data-centric collaboration. Access controls for devices such as laptops, hard disks, USB sticks etc. are mentioned [TM13].

The practice based on a **generic model hiding usage parameters** is very specific for data-centric collaborations and no related work could be found in regard to knowledge

protection. In general, this behaviour fits with the strategy to hide details mentioned in the literature [MTM15].

The **legal measures** are mentioned by several of the interviewees, but they are also aware of their limitations. Examples are measures like non-disclosure agreements, contractual clauses with suppliers, or competitor clauses. The pertinent literature also found that these measures are considered as relatively ineffective as their character is rather punitive [No01], that social control might be more effective than legal recourse [Li97], and that it is difficult and costly to enforce such legal measures [OHH11].

PRACTICE	LITERATURE COVERAGE
Practice 1: **Restrictive Partner Selection** Select less risky partners for collaboration and no close collaboration with critical partners.	Literature mentions restriction to groups [MTM15].
Practice 2: **Communication through Gatekeeper** Communication with partners via a single responsible person fully aware of knowledge risks.	Persistent participation to control knowledge risks [JV16], but not explicitly the role as control mechanism.
Practice 3: **Limit Access to Central Platform to a Small Number of People** Project-internal data exchange platform: only few representatives have access as a safety measure for secure sharing.	Defining role-based access models and as part of a social media strategy this can be used to control knowledge outflows [TM13] [Th14] [STM15].
Practice 4: **Hide Details of Machine Data Dumps** Details of machine data are hidden not to reveal implicit knowledge.	Share general knowledge & protect details [MTM15], but without specific focus on sharing data dumps.
Practice 5: **Data Won't Leave Factory for Analysis** Physical limitation: data must not leave the factory.	Access controls for devices such as laptops, hard disks, USB sticks etc. are mentioned [TM13], but not in regard to remote data analytics.
Practice 6: **Generic Model Hiding Usage Parameters** Model (of reactor processes) is created in a very generic and parameterizable form. Company partner executes it with secret process parameters which hence stay hidden for the scientific partner.	The strategy to hide details is mentioned in the literature [MTM15], but the application of a generic model for knowledge protection is not mentioned so far.
Practice 7: **Apply Legal Measures** Legal measures are applied to avoid unintended knowledge leakage or usage by sharing partners.	Frequently mentioned in literature, but relatively ineffective [No01] [Li97] [OHH11].

Table 3: Overview of the seven practices presented in detail.

Summing up, the practices restrictive partner selection, limiting access and apply legal measures are in line with the related work. The practice communication through gatekeeper is not mentioned as an explicit control mechanism so far. The practices hide details of machine data dumps, data won't leave factory and the generic model are specific

to data-centric collaborations and are not mentioned in the related knowledge protection literature so far, even if some general concepts like hide details are mentioned of course.

6 Conclusions

With the present work, we contribute the following to existing research on knowledge sharing and protection in knowledge sharing networks: Firstly, based on our overall impression from the carried out interviews, we confirm that there is a need for knowledge-intensive companies to participate in knowledge sharing networks. We also confirm that most individual representatives see this benefit. In parallel however, they struggle with how, practically, to protect sensitive knowledge in co-opetitive settings. In the setting that we investigated, the competitive and knowledge-intensive nature of the sector, knowledge protection was a significant concern in relationship to collaboration. Secondly, we would therefore suggest to call such a co-opetitive collaboration structure a "knowledge sharing and protection network", in which what is shared, and what is protected is carefully and tediously balanced in day-to-day collaborative activities. This added "and protection" in the name would acknowledge and appreciate the amount of effort made by the organisational representatives that goes into maintaining the necessary balance.

Finally, at the core of the paper we elaborated on seven distinct knowledge protection practices, based on 30 interviews. We could relate 3 practices well to prior literature, one partly and we note that 3 practices are not well covered by the knowledge protection literature as they are focussing specifically on data-centric collaborations. Practice 6 is unseen in literature, and as a third contribution of this paper we therefore provide this practice as newly enabled by data-driven technologies, and will also follow up on this practice in own future work.

Acknowledgements
The work has been performed in the project *Power Semiconductor and Electronics Manufacturing 4.0* (SemI40), under grant agreement No 692466. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal and Electronic Component Systems for European Leadership Joint Undertaking (ECSEL JU). The Know-Center is funded within the Austrian COMET Program – Competence Centers for Excellent Technologies – under the auspices of the Austrian Federal Ministry of Transport, Innovation and Technology, the Austrian Federal Ministry of Economy, Family and Youth and by the State of Styria. COMET is managed by the Austrian Research Promotion Agency FFG.

References

[BS01] Bloodgood, J.M. and Salisbury, W.D. 2001. Understanding the influence of organizational change strategies on information technology and knowledge management strategies. Decision support systems, 31(1), pp.55-69.

[GJ11] Gnyawali, D. R. and Park, B.-J. 2011. Co-opetition between giants: Collaboration with competitors for technological innovation. Research Policy 40, 5 (2011), 650–663.

[HST15] Hernandez, E., Sanders, W. G. and Tuschke, A. 2015. Network defense: pruning, grafting, and closing to prevent leakage of strategic knowledge to rivals. Academy of Management Journal, 58, 1233-1260.

[ITM18] Ilvonen, I., Thalmann, S., Manhart, M. and Sillaber, C. 2018. Reconciling digital transformation and knowledge protection: a research agenda. Knowledge Management Research & Practice, 16(2), 235-244.

[JM16] Jarvenpaa, S. L. and Majchrzak, A. 2016. Interactive self-regulatory theory for sharing and protecting in interorganizational collaborations. Academy of Management Review 41, 1 (2016), 9–27.

[JV16] Jarvenpaa, S. L., and Välikangas, L. 2016. "From governance void to interactive governing behaviors in new research networks." Academy of Management Discoveries 2, no. 3 (2016): 226-246.

[La08] Larsson, A., Ericson, Å., Larsson, T. and Randall, D. 2008. Engineering 2.0: Exploring Lightweight Technologies for the Virtual Enterprise. In Proceedings of the 2008 International Conference on the Design of Cooperative Systems. 205–216.

[LLP03] Levy, M., Loebbecke, C. and Powell, P. 2003. "SMEs, co-opetition and knowledge sharing: the role of information systems." European Journal of Information Systems 12.1 (2003): 3-17.

[Li97] Liebeskind, J. P. 1997. "Keeping Organizational Secrets: Protective Institutional Mechanisms and Their Costs," Industrial and Corporate Change (6:3), pp 623-663.

[LFP16] Loebbecke, C., van Fenema, P. C. and Powell, P. 2016. Managing inter-organizational knowledge sharing. Journal of Strategic Information Systems 25, 1 (2016), 4–14.

[Lu07] Luo, Y. 2007. A coopetition perspective of global competition. Journal of World Business 42, 2 (2007), 129–144.

[MT15] Manhart, M. and Thalmann, S. 2015. Protecting organizational knowledge: a structured literature review. Journal of Knowledge Management 19, 2 (2015), 190–211.

[MTM15] Manhart, M. and Thalmann, S. and Maier, R. 2015. "The Ends of Knowledge Sharing in Networks: Using Information Technology to Start Knowledge Protection". ECIS 2015 Completed Research Papers. Paper 129.

[Ma14] Mayring, P. 2014. "Qualitative content analysis: theoretical foundation, basic procedures and software solution." (2014): 143.

[Mo09] Montgomery, D. C. 2009. Design and analysis of experiments, 5th edn. John Wiley & Sons, Inc., New York.

[Non94] Nonaka, I. 1994. A Dynamic Theory of Organizational Knowledge Creation, Organization Science, 5(1), pp. 14-37

[No01] Norman, P. M. 2001. "Are Your Secrets Safe? Knowledge Protection in Strategic Alliances," Business Horizons (44:6), pp 51-60.

[OHH11] Olander, H., Hurmelinna-Laukkanen, P., and Heilmann, P. 2011. "Do SMEs Benefit From HRM-Related Knowledge Protection In Innovation Management?," International Journal of Innovation Management (15:3), pp 593-616.

[PMW15] Pahnke, E., McDonald, R., Wang, D. and Hallen, B. 2015. Exposed: Venture capital, competitor ties, and entrepreneurial innovation. Academy of Management Journal, 58, 1334-1360.

[Ri15] Ritala, P., Olander, H., Michailova, S., and Husted, K. 2015. "Knowledge sharing, knowledge leaking and relative innovation performance: An empirical study." Technovation 35 (2015): 22-31.

[STM15] Sarigianni, C., Thalmann, S., & Manhart, M. (2015). Knowledge risks of social media in the financial industry. International Journal of Knowledge Management (IJKM), 11(4), 19-34.

[SCK11] Spithoven, A., Clarysse, B. and Knockaert, M. 2011. Building absorptive capacity to organise inbound open innovation in traditional industries. Technovation 31, 1 (2011), 10–21.

[TI18] Thalmann, S., and Ilvonen, I. 2018 "Balancing Knowledge Protection and Sharing to Create Digital Innovations." Knowledge Management in Digital Change. Springer, Cham, 2018. 171-188.

[TM13] Thalmann, S., and Manhart, M. 2013. "Enforcing organizational knowledge protection: an investigation of currently applied measures." In Seventh (pre-ICIS) Workshop on Information Security and Privacy (WISP), Milan, Italy.

[Th14] 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 (IJKM), 10(2), pp.28-42.

[TS18] Thalmann, S., and Schäper, S. 2018. "Localizing Knowledge in Networks of SMEs – Implication of Proximities on the IT Support." Knowledge Management in Digital Change. Springer, Cham, 2018. 189-206.

[TD12] Trkman, P. and Desouza, K. C. 2012. Knowledge Risks in Organizational Networks: An Exploratory Framework. Journal of Strategic Information Systems 21, 1 (2012), 1–17.

7 APPENDIX

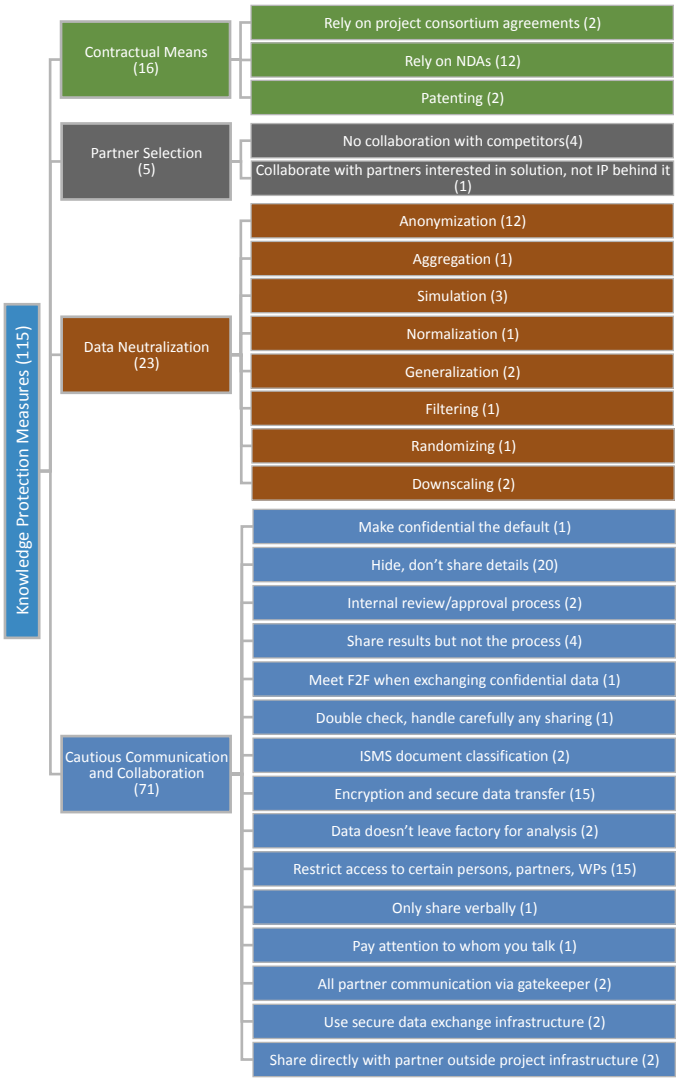

Figure 1: The 27 knowledge protection measures mentioned by the interviewees, grouped along 4 knowledge protection practices.