4.1 Knowledge risks in supply chain interactions of SMEs: An exploratory study

Klaus North[24], Armindo Barbosa de Carvalho[25]; Alessio Maria Braccini [26], Susanne Durst[27], João Alvaro Carvalho[28], Karin Gräslund[29], and Stefan Thalmann[30]

Abstract: Due to digitalization organizations increasingly interact with other organizations. Data, information, and knowledge are exchanged along the supply chain. This not only creates benefits but also creates manifold risks. The latter is particularly relevant for SMEs being usually the weaker partner in vendor buyer relations. This paper explores knowledge risks associated with supply chain interactions. Risks are identified for three phases of a typical vendor and buyer relations cycle: the preparation phase, the development and learning phase, and the operational phase. The relevance of the relations presented will have to be empirically validated. For this, explorative focus groups involving SMEs from Portugal and Italy were conducted. The overall aims of the ongoing research project are first, to raise awareness among SMEs about these risks, and secondly, to provide training and assistance for these companies on how to avoid or mitigate these risks.

Keywords: supply chain, risks, SMEs, knowledge risks, cyber risks

1 Introduction

Due to digitalization companies are increasingly pushed into cross-organizational collaborations. Consequently, an increasing amount of data, information, and knowledge is exchanged along the supply chain. According to [Ch98], a supply chain '...is a network of organizations that are involved, through upstream and downstream linkages in the

[24] Wiesbaden Business School, Hochschule RheinMain, Bleichstr.44, 65183 Wiesbaden; Klaus.North@hs-rm.de,

[25] Cotec, Edifício Porto INOVA,Rua Engenheiro Ferreira Dias, n.º 728 - Sala 1.05, P-4100 –246 Porto, armindo.carvalho@cotec.pt

[26] Università degli Studi della Tuscia, Via del paradiso, 47 - 01100 Viterbo, abraccini@unitus.it

[27] School of Business, University of Skövde, Högskolevägen, 541 28 Skövde (Sweden); susanne.durst@his.se

[28] Departamento de Sistemas de Informação, Universidade do Minho, P-4800-058 Guimarães Portugal; jac@dsi.uminho.pt

[29] Wiesbaden Business School, Hochschule RheinMain, Bleichstr.44, 65183 Wiesbaden, Karin.Graeslund@hs-rm.de

[30] Karl-Franzens-Universität Graz, Center for Business Analytics and Data Science 8010 Graz, Attemsgasse 11, stefan.thalmann@uni-graz.at

different processes and activities that produce value in the form of products and services in the hand of the ultimate consumer.'

The exchange of data, information, and knowledge along the supply chain can be viewed as one of the key characteristics of advanced manufacturing concepts, frequently labeled as industry 4.0 or advanced manufacturing [Ka15]. Data analytics promise huge advantages for supply chain management, especially in regard to quality management and for predictive maintenance. However, the exchange across organizational boundaries bears also the risks of losing competitive knowledge or of revealing business insights to other companies or even to competitors [MT15]. Further, the increasing digitalization of supply chains imposes also the risks of being in the focus of cyber-attacks [SLT15]. Both threats (1) not to know which business insights or critical knowledge an external part can derive from shared data and (2) to be a possible target of a cyber-attack, are major concerns of organizations in general.

Even though they belong to a heterogeneous universe of economic actors [NV16], small and medium enterprises (SMEs) are typically in a weak position when it comes to information and/or knowledge exchange relationships with larger firms and they are less able to deal with knowledge risks [LLP03]. Further, SME´s address knowledge protection mostly with informal measures and they have typically no systematic approach [MTM15]. This is because SMEs in contrast to large enterprises typically do not have the resources and especially the skills to react suitably to these risks [FH15]. Due to this situation, SMEs might be cautious about adopting digital technologies and/or they do not address or inadequately act towards the arising risks.

2 Linking knowledge risks to supply chain interactions

In a business context, risk expresses the fear that economic activities lead to the loss or devaluation of an important asset or a decrease in the performance of the business [HCN15]. Extant literature mainly relates supply chain risk to the probability of occurrence of disruptive events in the operational supply chain [HCN15]. There are only a few sources regarding strategic issues [St05] and knowledge as a risk factor is not addressed explicitly in the literature reviewing supply chain risks [GS15].

Durst and Zieba [DZ18] define knowledge risk as "a measure of the probability and severity of adverse effects of any activities engaging or related somehow to the knowledge that can affect the functioning of an organization on any level." This definition embraces also risks related to data and information. Those authors [DZ18] have also proposed a concept map of knowledge risks, which is viewed as a basis for more research at both the conceptual and empirical levels. Additionally, Ilvonen and colleagues [ITM18] identify knowledge risks in supply chains as one promising research avenue in the field of knowledge protection.

In the following, we will explore knowledge risks related to typical supply chain interactions. As to date there is no comprehensive taxonomy of supply chain interactions, the taxonomy below (see Table 1) has been compiled from different literature resources (e.g.

[MZ00], [SWS02], [St05]) as well as own action research and consulting activities the authors have done with actors in supply chains.

In order to reach our aim, we analyzed a typical cycle of vendor and buyer relations, [FF14] which we divided into three phases: the preparation phase, the development and learning phase, and the operational phase. The relations presented in Annex 1 will have to be empirically validated in the next step. For this, a focus group approach involving SMEs is envisaged. The main aims of the ongoing research project are first, to raise awareness among SMEs about these risks and second, to provide them training and assistance on how to avoid or mitigate these risks.

Let us now look into widespread knowledge risks in each of the three phases.

The preparation phase usually begins with a request for information followed by bidding and tendering or supplier rating. In the sales process, representing a sub-phase, suppliers are requested by clients to disclose financial data as a basis to agree on "allowed" margins, a common practice in the automotive industry. In this first phase, suppliers are required to disclose detailed information so that potential buyers can learn about the supplier's capabilities. This might lead to the undesired disclosure of competitive knowledge.

In the development and learning phase, suppliers innovate together with clients. New knowledge is created and often supplier staff is integrated into client teams. This collaborative process in a supply chain context may result in changes to the products, processes, or services [RSW04]. In this interaction, intellectual property (IP) protection poses considerable challenges [MCM13]. This is particularly true when engineers of the suppliers are integrated into client teams. There is also the risk that these persons defect to the client. In vendor building programs vendors, on the one hand, learn from clients but, on the other hand, must also be prepared to share their knowledge with performance improvement teams from clients or within a vendor network. This might lead to an undesired disclosure of critical knowledge.

The operational phase is characterized by an exchange of huge amounts of data and information and also involves ongoing decisions, operational order processing, and logistics processes. In this phase, there are a number of risks relating to people defecting and undesired disclosure of information.

Depending on the interaction modes used, e.g. EDI, online platforms and applications as well as cloud services cyber risks are also increasingly present. According to the US. National Institute of Standards and Technology (NIST) Key Cyber Supply Chain Risks include risks from third party service providers or vendors – from janitorial services to software engineering with physical or virtual access to information systems, software code or IP. Risk further include poor information security practices by lower-tier suppliers or compromised software or hardware purchased from suppliers. Software security vulnerabilities in supply chain management or supplier systems; counterfeit hardware or hardware with embedded malware constitute additional risks. Third party data storage or the use of data aggregators can also lead to serious knowledge risks.

3 Exploratory Study on Knowledge Risks in SMEs

The literature review on knowledge risks in supply chain interactions produced interesting results, but with no specific focus on SME´s. Based on this insight, we decided to conduct an exploratory investigation on how SMEs perceive knowledge risks in supply chain interactions in Portugal and Italy.

3.1 Data collection description

For this purpose, we collected data from representatives from SMEs in a workshop in Portugal and with interviews in Italy. Following a purposeful sampling approach, an invitation was sent to representatives of several SMEs engaged in cross-organizational supply chain interactions. Against our perception that issues related to information are often assigned to IT managers, we sought a mix of general managers and IT managers in the workshop. For the Portuguese SMEs invitations were made through personal contacts to enterprises that regularly participate in the activities promoted by COTEC - a Portuguese enterprise association to foster innovation. Although eight SME from the north of Portugal agreed to participate in the workshop, only four showed up for the workshop. All the no-shows were general managers (CEOs or equivalent). Thus, the workshop was run only with IT managers. All participants were male and had more than 10 years of professional experience. Besides the invitees, three other persons participated in the workshop: a project manager from COTEC and a researcher and a research assistant on IS. They acted as conductors of the session, moderators and they took notes of what happened in the workshop.

For the Italian SMEs invitations were sent through personal contacts to enterprises active in value chains in the Lazio region (center of Italy). The invitations turned in to six interviews with as many SMEs active in different value chains in the manufacturing industry. The interviews were performed with different managers: IT managers (for all companies), CEO (for two companies), and CPO (for two companies). All participants were male and had more than ten years of professional experience. All interviews were performed by a researcher and a research assistant who conducted the interviews took notes of what happened and transcribed the interviews afterwards.

Both the workshop with Portuguese SMEs, and the interviews with Italian SMEs consisted of three phases: inception, discussing, and closing. In the first phase, participants were confronted with a presentation that addressed information security in general and the key insights from the literature review (table 1). The discussion phase encompasses the testimonies of the participants. Participants were encouraged to share the practices of their enterprises and their technical opinions regarding the issues addressed. In the closing phase, the moderators brought up the aspects that emerged as more controversial or that were viewed as more important and asked the participants to confirm their viewpoints. The workshop lasted for around 90 minutes. The interviews lasted from a minimum of 40 mins to a maximum of 80 minutes. After the data collection, the moderators collated their notes and produced a summarizing report. The evidence of the data collected was eventually discussed among all the authors of this paper.

3.2 Data collection results

The results reported in this section are based on the discussions of the summarizing reports produced by the moderators of the workshop and interviews.

A first aspect to mention is that issues related to information and knowledge are perceived by the enterprises as belonging to the IT realm. When inviting enterprises to participate in the workshop, some managers suggested being represented by their IT managers. Furthermore, the general managers that agreed to be present ended up by not showing up. The discussions during the workshop somehow supported this. The participants, that stated to be well aware of their enterprise's actions, mainly reported protective measures related to computer security and with information and knowledge protection. The participants also mentioned that even though the general management is aware of security and knowledge risks, they view it as a cost they would like to avoid as much as possible and thus the IT managers have to go through great efforts to convince managers to the importance of such issues. In a few cases, this translated into the security management being completely outsourced to external technical personnel that provides basic security protection (hardware and software), and basic data backup and restore facilities.

Although all the interviewees in the session were aware of information and computer security, some of them reported that their awareness was raised after being victims of ransomware attacks. Furthermore, General Data Protection Regulation also contributed to raise the awareness to the need of paying more attention to protection issues, both from the perspective of potential victims of cyber-attacks, from the perspective of holders of information about their customers, and from the perspective of the implications of being accountable of the consequences of data breaches targeting information of customers and business partners. However, most of the security measures address access to computers, only a few to protect knowledge.

Bidding and tendering are not perceived as risky moments for sensitive information and knowledge. The perception of the workshop participants is that these activities involve mostly administrative information. Therefore, no special care needs to be taken with the corresponding interactions. This doesn't mean that the enterprises are naive in their commercial relations. They value trust and whenever they perceive a supplier or customer as non-trusting, they avoid them.

If security procedures (technical or non-technical) become obtrusive and affect easy access to information by the parties, such procedures are likely to be rejected by management. Similar attitude exists regarding the information sales people have to deal with. Although management is aware of the risk of losing competitive knowledge related to their customers, they privilege easy access to information by sales people instead of establishing extra protection measures.

Investing in education and training is crucial to protect the company's knowledge, especially on non-technical people. Social engineering is one of the major threats to the companies, and the employees must be informed of all the risks. For instance, one participant said "If there is an email with "invoice" in the subject, the email will be open by the

accounting personnel". Another treat perceived by SMEs originates in the potential misuse of personal devices within the company network, or company device assigned to employees within their personal (back home) IT environment. For instance, two SMEs from Italy reported having security problems with ransomware attacks diffused from IT devices infected from personal e-mails received by employees on their computer at work. They recognize weaknesses in what concerns the companies' digital competences of most employees, including those that deal with sensitive information and knowledge. The SMEs stressed also the need to strengthen digital competences and leadership in HR for future development of IT deployment within the organization.

All the participants referred that is inevitable to work in supply chain networks. When they work with large companies, they accept the security requirements they impose. Such requirement might include going through audits, signing non-disclosure agreements regarding the information of the products they manufactured, or other. However, the participants don't have the same procedure with their suppliers, normally smaller companies that they perceive as not being prepared to deal with demanding protection measures.

Some companies have shown some apprehension about losing critical knowledge to competitors. But at the same time, they have not pointed out a clear strategy for mitigating such concerns. The risk of losing knowledge is faced as a normal risk of the business, and they will not refrain to accept a contract because of fear of losing knowledge. When working on supply chain networks, they provide all the information that is asked, as they view that as inevitable if they want to participate in these supply-chain networks. Two SMEs acknowledged during the interviews that they are under the risk of potential knowledge spillover to their technology provider which supplies hardware and software for the automation of the assembly line. However, their reaction is ambivalent because in one case they believe the data being stolen would not constitute a risk for them and hence do not perceive the risk need to be mitigated, in another case they acknowledge the risk of losing competitive advantage, but this risk is neither quantified nor protected.

The companies seem to protect their intellectual property as much as necessary to be in a fair market. When competitors are not fair, there isn't much they can do about it. Some of the companies have patents and are aware that it is easy (and likely) that their products are copied. However, the costs of protection and the time it takes to solve those issues lead them not to worry too much with copyright infringement situations. Some companies consider that the patents do not give them a special position in the market, instead, they rely on building strong relationships with clients and suppliers, and in the quality of the goods, they manufacture or of the services they provide.

The R&D&I area is the most protected area of the company and the one that has more valuable information, however, there is no estimation of the value of this information, no list of risks of losing this information and no assessment of the risks of having a cyber-attack.

4 Conclusions and outlook

Our results show and ambivalent behavior of our interviewees. One the one hand they are aware of the risks of losing competitive knowledge to a certain extent and on the other hand they do not care if it comes to supply-chain interactions (in particular) with large enterprises. One of the major reasons for this is a lack of awareness about the multitude of knowledge risks that may emerge in supply chain interactions and about possible countermeasures. Second, our interviewees highlighted missing technical skills on how to protect knowledge in a digitized supply chain. Hence, there is a need for awareness training for organizations in supply chains, particularly for SMEs. This training should help in developing greater transparency which would benefit not only the companies' owners/owner-managers but also the entire supply chain management. Additionally, the training should also focus on digital skills regarding the protection of knowledge. Policy makers may also benefit from this improved transparency and could, in turn, offer better support and assistance

Another remarkable insight was the pragmatism regarding large enterprises. Even if the companies realize that they are losing competitive knowledge, they fulfill the requirements from the largen enterprises to get the contract. The SMEs describe the pressure from the large enterprises and the more equal sharing interaction with another SME. From our perspective, there is a need to investigate this relationship in more detail and to start a policy making process.

In this ongoing research project, we have made the first step to explore knowledge risks in supply chain interactions. In our explorative investigation, it turned out that SMEs are under strong pressure from large enterprises and that they do not have the skills and the resources to take suitable measures. The findings are limited to the workshop and interviews in Portugal and Italy and will need to be confirmed by a larger sample of firms. Based on the insights gained the involved research team will consider how to raise awareness about the risks and assist SMEs in avoiding or mitigating the risks according to their needs.

Literature

[Ch98] Christopher, M.: Logistics and Supply Chain Management. Strategies for Reducing Cost and Improving Service. Second ed. London, 1998

[DZ18] Durst, S., & Zieba, M.: Mapping knowledge risks: towards a better understanding of knowledge management, Knowledge Management Research & Practice, DOI: 10.1080/14778238.2018.1538603,2018

[ED14] Edvardsson, I.R., & Durst, S.: Outsourcing of knowledge processes: a literature review. Journal of Knowledge Management, 18(4), 795-811, 2014

[FH15] Falkner, E.m. Hiebl, M.: "Risk management in SMEs: a systematic review of available evidence", The Journal of Risk Finance, Vol. 16 Issue: 2, pp.122-144, 2015

[FF14] Fraser Johnson, P; Flynn, A.: Purchasing and Supply Management. McGraw-Hill Education; 15th Edition, 2014

[GS15] Guertler, B. & Spinler, S. (2015) Supply risk interrelationships and the derivation of key supplyrisk indicators. Technological Forecasting & Social Change 92, 224–236. https://doi.org/10.1080/14778238.2018.1538603.

[HCN15] Heckmann, I., Comes, T., Nickel, S.: A critical review of supply chain risk – Definition, measure, and modeling. Omega 52, 119–132, 2015

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

[Ka15] Kagermann, H.. "Change through digitization—Value creation in the age of Industry 4.0." Management of permanent change. Springer Gabler, Wiesbaden, 2015. 23-45.

[LLP03] Levy, M.; Loebbecke, C.; Powell, P: SMEs, co-opetition and knowledge sharing: the role of information systems. In: European Journal of Information Systems 12 (1), S. 3–17. DOI: 10.1057/palgrave.ejis.3000439, 2013.

[MT15] Manhart, M., and S. Thalmann. "Protecting organizational knowledge: a structured literature review." Journal of Knowledge Management 19.2: 190-211, 2015.

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

[MZ00] Min, H.; Zhou: Supply chain modeling: past, present, and future. Computers & Industrial Engineering 43, 231- 249, 2002

[MCM13] Mueller, E., Cockburn, I.M., MacGarvie, M.: Access to intellectual property for innovation: Evidence on problems and coping strategies from German firms, Research Policy, 42(2), 529-541, 2013

NIST (no year): Workshop brief on cyber supply chain best practices. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

[NV16] North, K. Varvakis, G. Eds: Competitive strategies for small and medium enterprises. Heidelberg: Springer, 2016

[RSW04] Roy, S., Sivakumar, K., Wilkinson, I.F.: Innovation Generation in Supply Chain Relationships: A Conceptual Model and Research Propositions. JOURNAL OF THE ACADEMY OF MARKETING SCIENCE, winter 2004, pp. 61-78, 2004

[SWS02] Simatupang, T.M. Wright, A.C., Sridharan, R.: The knowledge of coordination for supply chain integration. Business Process Management Journal, Vol. 8 No. 3, pp. 289-308, 2002

[St05] Stadtler, H.: Supply chain management and advanced planning—basics, overview, and challenges. European Journal of Operational Research 163 (2005) 575–588, 2005

[SLT15] Stjepandić, J., H. Liese, and AJC Trappey : Intellectual property protection" Concurrent Engineering in the 21st Century. Springer, Cham, 521-551, 2015.

[WD18] Williams, C., & Durst, S.: Exploring the Transition Phase in Offshore Outsourcing: Decision Making amidst Knowledge at Risk. Journal of Business Research, https://doi.org/10.1016/j.jbusres.2018.01.013, 2018

Annex 1: Knowledge risks in supply chain interactions

Type of interaction	Description	Knowledge risk	References
The preparation phase			
Bidding and tendering, Requests for information	In the offer and tendering process suppliers are requested to provide detailed technical information, project references etc.	Disclosure of competitive knowledge	[MTM15]
Sales process	Sales reps of suppliers develop privileged relations with clients and accumulate knowledge about clients	Sales representatives defect and take clients with them	
Supplier/vendor rating	Vendors/ suppliers are given standing, status, or title according to their attainment of some level of performance and capabili-	Disclosure of competitive knowledge	[MTM15]

	ties.		
Open book interaction	Suppliers are requested by clients to disclose financial data as a basis to agree on "allowed" margins	Disclosure of competitive knowledge	
The development and learning phase			
Collaborative product and service development	Suppliers innovate together with clients, new knowledge is created Supplier staff is integrated into client teams	Unclear IP protection, The expertise of suppliers is used by clients without adequate compensation	[RSW04]
Project development and execution by supplier consortium	Suppliers collaborate and pool resources to win and execute multifaceted projects	Disclosure of competitive knowledge, unwanted knowledge spill-over	
Vendor building	Vendors learn from clients but have to share knowledge with teams from clients or within a vendor network, development of global outsourcing relationships	Disclosure of competitive knowledge	[WD18]
The operational phase			
Advanced supply chain planning	Exchange of market and capacity information along the supply chain	Disclosure of knowledge on market position, plans, strategies and performance	[St05]
Job shops or contract manufacturing	Clients supply material and often also equipment and suppliers execute work according to the clients' detailed specifications	Dependency on know-how of client and total transparency of performance	

Operational order fulfilling, and logistics processes and ongoing decisions made in a client-vendor arrangement	These processes often require a close interaction, information and data exchange between supplier and client	Unwanted knowledge spill-over personnel from supplier defects to clients	
Division of labour	Focus on core competences	Unlearning, knowledge attrition and knowledge loss	[ED14]
Interaction modes via EDI, online platforms and applications, cloud services etc.	Depending on the modes of interaction used data, information and knowledge are exchanged, Lack of state of the art technology, software etc.	Undesired disclosure or loss of data, information, and knowledge, Risk of hacker/cyber-attacks, risks related to the application of old technologies/software, espionage	NIST, [DZ18]