MASTER’S THESIS

Johanna Orjatsalo 2020

LAPPEENRANTA-LAHTI UNIVERSITY OF TECHNOLOGY LUT
SCHOOL OF BUSINESS AND MANAGEMENT
KNOWLEDGE MANAGEMENT AND LEADERSHIP

Johanna Orjatsalo

KNOWLEDGE CREATION IN CYBERSECURITY THREAT MODELING WORKSHOPS – CASE STUDY

Master's thesis 2020

Examiners 1st examiner: Professor Kirsimarja Blomqvist
2nd examiner: Post-doctoral Researcher Argyro Almpanopoulou

ABSTRACT
Lappeenranta-Lahti University of Technology LUT
School of Business and Management
Degree Programme in Knowledge Management and Leadership

Johanna Orjatsalo

KNOWLEDGE CREATION IN CYBERSECURITY THREAT MODELING WORKSHOPS – CASE STUDY

Master's Thesis
2020
137 pages, 20 figures, 4 tables and 5 appendices

Examiners 1st examiner: Professor Kirsimarja Blomqvist
2nd examiner: Post-doctoral Researcher Argyro Almpanopoulou

Keywords knowledge, knowledge management, knowledge creation, social capital, shared context, knowledge combination, knowledge exchange, SECI, cybersecurity, threat modeling, technology architecture, workshop

Understanding all the levels of the whole technology stack of an organizational entity, all its interfaces, and how it works in practice is often challenging. Still, organizations need to be capable to examine their digital operations from different angles whenever needed. To cope with the fact that they might not have adequate and up-to-date knowledge easily available, organizations have developed various approaches to pull together required knowledge of their digital operations for certain purposes.

This research focused on examining knowledge creation as part of one of those approaches, cybersecurity threat modeling workshops. The objective of this qualitative case study was to form an understanding about the enablers of knowledge creation during threat modeling, and especially how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context.

Research material consisted of three cases, each representing a threat modeling workshop having different scope and participants. Empirical data was gathered by observing the threat modeling workshops and interviewing the respective facilitators and owners for each case. Various knowledge management theories and concepts were used both for designing the research as well as reflecting the observations and findings.

The study identified several elements and aspects that were considered to impact knowledge creation both before and during threat modeling workshops, and which could be linked to the existing knowledge management theories and concepts. Additionally, it produced some practical observations that can be used for developing threat modeling practices going forward.

TIIVISTELMÄ

Lappeenrannan-Lahden Teknillinen Yliopisto
School of Business and Management
Tietojohtamisen ja johtajuuden koulutusohjelma

Johanna Orjatsalo

KNOWLEDGE CREATION IN CYBERSECURITY THREAT MODELING WORKSHOPS – CASE STUDY

Pro gradu -tutkielma
2020
137 sivua, 20 kuvaa, 4 taulukkoa ja 5 liitettä

Tarkastajat 1. tarkastaja: Professori Kirsimarja Blomqvist
2. tarkastaja: Tutkijatohtori Argyro Almpanopoulou

Hakusanat tieto, tietojohtaminen, tiedon luominen, sosiaalinen pääoma, jaettu konteksti, tiedon yhdistäminen, tiedonvaihto, SECI-malli, kyberturvallisuus, uhkamallinnus, teknologia-arkkitehtuuri, työpaja

Organisaatioiden on usein haastavaa ymmärtää digitaalisten järjestelmiensä muodostamaa kokonaisuutta, sen rajapintoja sekä käytännön toimintaa. Tästä huolimatta niiden on pystyttävä tarkastelemaan digitaalisia toimintojaan eri näkökulmista aina tarpeen mukaan. Organisaatiot ovatkin kehittäneet erilaisia tapoja muodostaa tietoa erilaisista järjestelmäkokonaisuuksistaan myös niissä tilanteissa, joissa tämänkaltainen tieto ei välttämättä olisi valmiiksi saatavilla.

Tämän tutkimuksen tavoitteena oli tarkastella tiedon luomiseen vaikuttavia tekjöitä edellä mainitun kaltaisessa tilanteessa: kyberturvallisuuteen liittyvien uhkamallinnustyöpajojen yhteydessä. Tutkimus toteutettiin laadullisena tapaustutkimuksena, ja sen tavoitteena oli ymmärtää, mitkä tekijät edesauttavat tiedon luomista uhkamallinnuksen yhteydessä sekä erityisesti sitä, onko organisaation sosiaalisella pääomalla tai tiedon luonteella mahdollisesti vaikutusta tiedon luomiseen.

Tutkimusmateriaali koostui kolmesta eri uhkamallinnustyöpajasta, joista kukin käsitteli eri sisältöä eri osallistujien voimin. Empiirinen tutkimustieto kerättiin tarkkailemalla työpajojen kulkua sekä haastattelemalla kunkin työpajan ohjaajaa sekä omistajaa. Tietojohtamisen teorioita ja konsepteja käytetiin abduktiivisesti tutkimuksen eri vaiheissa.

Tutkimus auttoi tunnistamaan sekä työpajatyöskentelyyn että työpajoja edeltäneisiin valmisteluihin liittyviä, tiedon luomiseen vaikuttavia elementtejä ja näkökulmia sekä löytämään yhteyksiä näiden elementtien ja tietojohtamisen teorioiden ja konseptien välillä. Näiden tutkimuslöydösten lisäksi tutkimus tuotti muutamia käytännöllisiä huomioita uhkamallinnuskäytäntöjen kehittämiseksi.

ACKNOWLEDGEMENTS

Back in 2005, I wanted to learn more about how neural networks work and started studying Information and Service Management at Aalto University. Finalizing the studies and working full time proved to be somewhat challenging, and at the beginning of 2018 I decided that I would need to do something about this. And then I found LUT University's program of Knowledge Management, TIJO <3

This Master's thesis is a result of many iterations, and while nearly everything has been changed at least once during this process, now it is time to let go and leave it as it is. I would like to thank all the following for making this possible:

- All the case organization representatives who were involved in this study, for providing the opportunity to closely monitor their threat modeling work and for sharing their insights so openly
- Antti Vähä-Sipilä and Laura Noukka for the ideas, sparring, discussions, and all
- Professor Kirsimarja Blomqvist from LUT University for making her valuable experience available throughout the journey
- TIJO2018 for first-class 24/7 peer support
- Alma Mater x 2 aka LUT University for the past 2 years and Aalto University for the past n-2 years
- COVID19 for the interesting changes of plans
- Taxpayers of Finland for the financial support available through Finnish Employment Fund (aikuiskoulutustuki)
- My dear friends, especially Inna, for mental support

And last but not least

- J, J & K for putting up with me and making sure I did not get too involved into this stuff (even though it was sometimes very very close)

22.7.2020

Johanna Orjatsalo

TABLE OF CONTENTS

FIGURES

TABLES

1 Introduction

Organizations are continuously developing their digital operations, and due to the high speed of this change, understanding all the levels of the whole technology stack of an organizational entity, all its interfaces, and how it works in practice has become challenging. Despite various models, methods and guidelines that have been developed for keeping track on the organization's digital architecture, major share of such knowledge is often not directly available or usable when needed. (Babar & Gorton 2007; Zimmermann et al. 2012; Schoenfield 2015; Capilla et al. 2016). To cope with the fact that they might not have the adequate knowledge easily available, organizations have developed various approaches to form an understanding of their digital operations for specific purposes whenever needed. This study looks at knowledge creation as part of one of those approaches, cybersecurity threat modeling.

1.1 Background for the study

Knowledge related to organization's digital and enterprise architecture is important for managing, developing, and improving its operations but also when evaluating and mitigating the potential risks. Similarly to physical operations, the risks of failure for digital operations are connected to those situations in which the system or its components do not contribute as intended, or in which there is a possibility that they can be altered to contribute in a different way than what was originally intended. The concept of "cybersecurity" can be seen as a combination of various activities that aim at securing different types of digital structures and objects (such as data, processes or devices) to prevent damage that can occur if these structures do not function as intended. These activities need to be in line with the constantly evolving digital architecture and the continuous interaction between various actors reforming this knowledge, as well as the continuously emerging and developing cybersecurity threat landscape. (Shostack 2014; Schoenfield 2015).

Organizations can apply various cybersecurity approaches and methods, aiming at either preventing the cybersecurity incidents from happening or minimizing the damage caused by them. End-to-end cybersecurity management approach is often considered to consist of four different categories of activities: 1) identify/predict the

risks/threats, 2) prevent them from happening by improving cybersecurity levels (defense), 3) detect possible threats/attacks/breaches, and 4) respond with fixes and further improvements. (Gartner 2017; National Institute of Standards and Technology (NIST) 2018).

From knowledge management point-of-view, cybersecurity activities have traditionally been considered as a mean of protecting the organization's intellectual capital and operations, which according to the Knowledge-Based View of the firm are the most important assets for the organization. Hence, it has been considered as a moderator of the organization's value creation process and knowledge management activities rather than one of those capabilities that would create competitive advantage. (Gold et al. 2001; Sallos et al. 2019)

Knowledge management literature includes several examples of research work that applies knowledge management related frameworks and concepts in value creating activities, such as innovation management, business ecosystems management or general management (Handzig 2017). It has been only recently that knowledge management has been brought up as a research field that could bring significant enhancement also into cybersecurity planning and management (Tisdale 2015). The examples include, e.g., evaluating possibilities to store and reuse cybersecurity related knowledge (Souag et al. 2016) or using knowledge management toolset to facilitate cybersecurity related knowledge creation (e.g., Kalogeraki et al. 2018).

Cybersecurity provides an interesting research context for knowledge management researchers for two reasons. First, even though the organizations would have a rather well-managed knowledge repository from architectural point of view, it alone does not serve the purpose of assessing or improving their security. Vast majority of the security issues emerge as a combination of several factors, and many of them also involve interaction of some kind, either between the systems or their components, between material and human actors, or even between humans alone. In cybersecurity planning and management, it is therefore typical that forming an understanding of threats for a certain part of a system requires exchanging and combining information and knowledge between different sources. (Schoenfield 2015)

Second, having adequate knowledge of digital operations and related risks, threats and vulnerabilities is not enough. To plan and manage its cybersecurity activities, an organization also needs to understand how to identify, prioritize and apply activities based on this knowledge. The dynamic and context-specific nature of (technology-related) knowledge in organizations creates challenges for identifying and applying adequate cybersecurity activities but also for managing the cybersecurity knowledge itself. In their article published at the end of 2019, Sallos et al. have defined cybersecurity management primarily as a knowledge problem, describing this problem as “knowledge about lack of cybersecurity knowledge within the boundaries of organization” (Sallos et al. 2019, 592). This lack of knowledge originates from the overall complexity and scattered nature of architectural knowledge within organizations, but also from the aspect that cybersecurity related knowledge is a specific area of knowledge, which is not that common within organizations in any format (Tisdale 2015; Sallos et al. 2019).

Cybersecurity risk management approaches, methodologies and frameworks provide an opportunity for organizations to understand, analyze and prioritize the risks attached to their digital structures and support them in creating mitigation plans. This study focuses on threat modeling, which is part of predictive cybersecurity activities. The objective of threat modeling is to increase the understanding what kind of threats can put a certain system and its operability under risk. The organization then uses this knowledge to decide their approach regarding the identified threats. (Shostack 2014; Schoenfield 2015; Gartner 2017, National Institute of Standards and Technology (NIST), 2018). Threat modeling can be done in numerous ways, and for this study, the research focus will be on three individual threat modeling workshops.

1.2 Research objectives and rationale

The main objective of this study is to understand the enablers of knowledge creation in the context of threat modeling workshops, and especially how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context.

As the study also serves as a Master’s thesis, it also has a secondary objective of providing the researcher with an opportunity to learn how knowledge management

research approaches knowledge creation. Depending on the relevancy of the research findings, the work can also provide new, practical ideas for developing threat modeling workshops and related practices from knowledge management perspective.

According to knowledge management researchers, knowledge is created through continuous interaction amongst human actors as well as between human and non-human actors (such as the physical environment). Knowledge is not the same as information; instead of being the same for everyone, it is subject to various individual-level meanings through interpretations made by everyone involved in the related interaction. To enable knowledge creation, knowledge needs to be shared/transferred; both knowledge combination and knowledge exchange are thereby crucial activities for knowledge creation. Knowledge-related interaction takes place even without intentional facilitation. However, it can be enhanced with intentional activities, such as improving the conditions for knowledge combination and exchange (Nonaka 1994; Spender 1996; Nahapiet & Ghoshal 1998; Cook & Brown 1999; Nonaka et al. 2000; Fong 2003).

When discussing the characteristics of cybersecurity related knowledge in organizations, the high speed of technological development and its impacts on the dynamic, uncertain, and context-specific nature of knowledge must be highlighted (Sallos et al. 2019). As discussed earlier in this chapter, knowledge needed for planning and managing cybersecurity related activities is often scattered and not easily available, and organizations typically need to involve stakeholders from different teams within an organization as well as from other organizations, such as third party vendors, in order to ensure they have access to adequate knowledge. (Schoenfield 2015; Tisdale 2015).

Cybersecurity threat modeling workshops are an excellent case example of intentionally facilitated knowledge creation within cybersecurity context. The scope for threat modeling (for example a system, a connection, a change, or a feature) is agreed prior to the workshop. During the actual workshop, the participants need to form a common understanding of the area included in the scope, and then work together on identifying the potential threats based on this knowledge. Having such a joint objective facilitates knowledge creation, and there are also various tools,

methods and guidelines that are being used to support this. (Shostack 2014, Schoenfield 2015)

1.2.2 Key definitions

This study discusses various definitions, many of which are explained as they are first introduced. However, there are a few key definitions which help defining the overall scope of the study.

Cybersecurity consists of activities to protect different types of digital structures and objects (such as data, processes, devices), to prevent damage that can occur if these structures do not function as intended. (Schoenfield 2015).

Knowledge is something we use for evaluating and incorporating new experiences and information. Creating and applying it requires human activity, and it consists of a mix of “framed experience, values, contextual information and expert insight”. In organizations, it exists in several formats, such as documents but also as organizational processes, routines and practices. (Davenport and Prusak 1998, 5).

Knowledge exchange means mutual sharing of knowledge between at least two actors, and it is a prerequisite for knowledge combination (Nahapiet & Ghoshal 1998, 248).

Knowledge combination involves creating new knowledge either through combining elements previously unconnected or by developing novel ways of combining elements previously associated (Nahapiet & Ghoshal 1998, 248).

Knowledge creation means renewing one’s existing context and knowledge through the continuous interaction with others, either other individuals or environment (Nonaka et al. 2000, 8). Knowledge is created through exchange and combination (Nahapiet & Ghoshal 1998, 248).

Social capital is formed by those resources that are included in or can be reached via the relationships of an individual or organization (social unit) to other individuals or organizations. (Nahapiet & Ghoshal 1998, 243).

Threat modeling is based on using abstractions to help understand what kind of threats can put organization’s digital operations under risk (Shostack 2014, xxiii).

1.2.3 Research questions

The main research question and its sub-questions are formed directly based on the research objective. The main research question is:

A. What enables knowledge creation in cybersecurity threat modeling workshops?

Addressing this question requires answering to the following sub-questions:

B. What is knowledge creation and how does it take place?
C. How do the different characteristics of knowledge impact knowledge creation?
D. How do the different aspects of social capital impact knowledge creation?
E. Which elements of knowledge creation can be identified in cybersecurity threat modeling workshops?

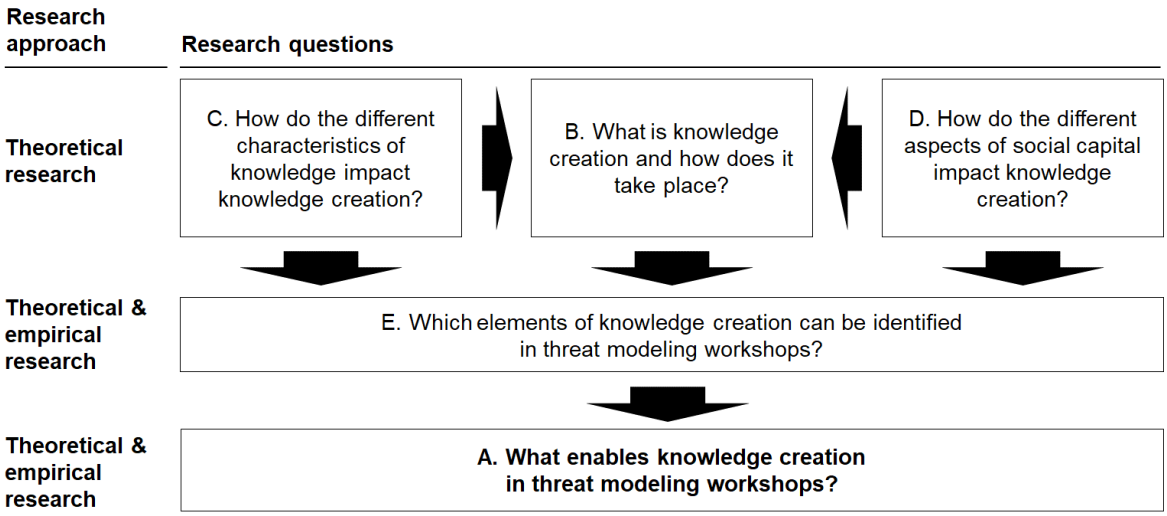


Figure 1. Research question, sub-questions and related research approach.

Figure 1 describes the connection between research questions and research approach. A theoretical research in the form of literature review is used for forming an understanding of knowledge creation (sub-question B) as well as the potential elements impacting knowledge creation (sub-questions C & D). Additionally, an empirical research is conducted to identify the potential elements of knowledge creation in threat modeling workshops (sub-question E), and to answer the main

research question on what enables knowledge creation in threat modeling workshops (question A).

1.2.3 Research focus and theoretical scope

This study assumes that both the fast pace of digitalization and the dynamic and context-driven nature of knowledge create additional challenges for planning and managing cybersecurity activities. Consequently, this creates a need for organizations to intentionally facilitate their knowledge creation to be able to plan and manage their cybersecurity-related activities. This assumption emerges from both the personal experiences of the researcher, as well as from cybersecurity related literature (Shostack 2014; Schoenfield 2015; Tisdale 2015; Sallos et al. 2019) and the research objective is strongly based on this assumption.

Knowledge management has always had strong connections to other sciences, such as library (and information management), computer (and information systems), cognitive and organizational sciences, and is also used as a methodology or tool on many of these fields. Some of the recent knowledge management research work indicates that knowledge management is shifting into a direction where it would experience a fusion with other disciplines. (Handzig 2017). As a Master's thesis, the secondary objective of this study is to learn about knowledge management theories and concepts, and for this purpose, the focus is on basic-level knowledge management theories and concepts, mostly excluding the potential further knowledge management research that has been done with a focus on for example the field of computer/information systems.

Earl (2001, 218) sees that knowledge management research has been conducted from three different positions: 1) technocratic school focuses on how information or management technologies support knowledge work, 2) economic school is interested in how knowledge and intellectual capital contribute to revenue generation, whereas 3) behavioral school examines how managers and management can facilitate knowledge creation, sharing and usage. Handzig (2017) has further categorized knowledge management research being related to three contexts: 1) knowledge enablers ("social and technical factors in enabling and facilitating knowledge processes"), 2) knowledge processes ("processes through

which knowledge is moved and modified"), and 3) knowledge stocks ("knowledge is seen as a valuable organizational asset", bringing together "different perspectives of knowledge").

In terms of the three knowledge management schools identified by Earl (2001), this study represents the behavioral school as it focuses on how knowledge creation takes place as a human interaction, and as part of this, examines the elements facilitating knowledge creation. As the research focus is strongly on the enablers of knowledge creation, this study does not describe knowledge creation as a process taking place during threat modeling workshops, nor provides a detailed narrative on how individual workshop participants contribute to knowledge creation activities.

Regarding knowledge enablers facilitating knowledge creation, the theoretical focus is more on social than technical factors enabling and facilitating knowledge creation. As knowledge creation is based on a combination and exchange of (existing) knowledge, also the nature of knowledge is examined as part of potential enablers and as a contextual factor. (Nonaka 1994; Nahapiet & Ghoshal 1998; Cook & Brown 1999; Nonaka et al. 2000).

Knowledge management theories and concepts relevant to this study are described in Table 1. Regarding the three research contexts defined by Handzig (2017), the analysis will include elements of all three: knowledge enablers, knowledge processes and knowledge stocks. From the process and stocks perspectives, the research is based on the viewpoint of knowledge being dynamic and context-specific, rather than looking at it as stock of knowledge or knowledge base (Nonaka 1994; Nonaka & Takeuchi 1995; Cook & Brown 1999; Nonaka et al 2000; Takeuchi & Nonaka 2002; Nonaka & Von Krogh 2009). It also considers knowledge being situated in organizations and individuals in many forms (Nonaka 1994; Blackler 1995; Spender 1996; Teece 1998; Cook & Brown 1999; Nonaka et al. 2000).

This study also adapts a dynamic view on knowledge creation, hence, it considers knowledge creation to take place as a continuous spiral rather than a linear process, or even a continuous state of "knowing", due to the dynamic and context-specific nature of knowledge (Nonaka 1994; Blackler 1995; Cook & Brown 1999; Nonaka et al. 2000; Alavi & Leidner 2001; Fong 2003; Pinho et al. 2012). Regarding

knowledge enablers, especially the role of social capital, its three dimensions and the four conditions of knowledge creation are discussed (Nahapiet & Ghoshal 1998). The theory of social capital role in knowledge creation is also compared with the role of shared context in knowledge creation (Nonaka 1994; Blackler 1995; Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003).

Table 1. Knowledge management theories and concepts relevant to this study.

Research sub-question	Key theories	Concepts	Examples of literature
C. How do the different characteristics of knowledge impact knowledge creation?	Nature of knowledge	Main dimensions of knowledge Different types of knowledge Dynamic nature of knowledge	Nonaka 1994; Blackler 1995; Spender 1996; Teece 1998; Cook & Brown 1999; Nonaka et al. 2000
B. What is knowledge creation and how does it take place?	Knowledge creation Social capital	Elements of knowledge creation Shared context Conditions for exchange and combination	Nonaka 1994; Blackler 1995; Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003 Nahapiet & Ghoshal 1998
D. How do the different aspects of social capital impact knowledge creation?	Social capital	Structural, relational and cognitive dimensions of social capital	Nahapiet & Ghoshal 1998; Adler & Kwon 2000; Lesser 2000

1.3 Research methodology and approach

The main objective of this study was to understand how knowledge creation takes place in threat modeling workshops, and how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context. The research was based on knowledge management theories and concepts, and it was conducted as a qualitative case study. Abductive reasoning logic was used as the analysis logic throughout the research. (Dubois & Gadde 2002; Blatter 2012; Timmermans & Tavory 2012). Empirical research material was gathered from three threat modeling workshops and analyzed as multiple case study. (Yin 2017).

The research assumptions described in section 1.2.3 acted as the basis for the abductive research design, in which the theoretical and empirical material was analyzed simultaneously. First, a literature review was conducted to identify initial answers to three of the sub-questions and to anticipate potential structure and methods for empirical data gathering. For this purpose, the theories of knowledge creation, nature of knowledge and social capital were examined (see Figure 2).

Initial findings from the literature review were then used to create an initial understanding of the theoretical base describing knowledge creation and its enablers.

Based on the initial theoretical base, the structure for the empirical research approach was designed with the objective of gathering data to answer the fourth sub-question: E. Which elements of knowledge creation can be identified in cybersecurity threat modeling workshops?

Empirical data was gathered from three cases (cybersecurity threat modeling workshops) as a qualitative inquiry. Primary research data was gathered through non-participant observations during the workshops as well as by conducting semi-structured interviews of workshop facilitator and owner before and after each workshop. Workshop presentations and documentation were used as secondary data to complement primary research data.

Data analysis started during data gathering and transcription by comparing the theories examined for literature review with the empirical observations. The actual data analysis was done after data gathering, and it included classifying the data and identifying potential connections between the observations and the potential set of theories and concepts. The outcomes of this comparison were used for enriching the set of theories and concepts discussed in literature review. Finally, the findings emerging from the data and their theoretical and conceptual linkages were used as the basis for the research discussion and conclusions. Research approach and structure are summarized in Figure 2.

Theoretical research: Literature review (Chapters 2, 3 and 4)

C. How do the different characteristics of knowledge impact knowledge creation?		B. What is knowledge creation and how does it take place?		D. How do the different aspects of social capital impact knowledge creation?	
Key theories	**Concepts**	**Key theories**	**Concepts**	**Key theories**	**Concepts**
Nature of knowledge	Main dimensions of knowledge Different types of knowledge Dynamic nature of knowledge	Knowledge creation Social capital	Elements of knowledge creation Shared context Conditions for exchange and combination	Social capital	Structural, relational and cognitive dimensions of social capital

Empirical research: Qualitative case study (Chapters 5 and 6)

E. Which elements of knowledge creation can be identified in threat modeling workshops?

Results, discussion & conclusions (Chapters 6 and 7)

A. What enables knowledge creation in threat modeling workshops?

Figure 2. Research approach and structure.

1.4 Research structure

Research structure follows the previously introduced research approach (Figure 2). Chapter 2 starts with a short introduction to knowledge management and then proceeds to describing the characteristics and nature of knowledge. After the introduction to knowledge and its nature, Chapter 3 approaches knowledge creation from the viewpoint of knowledge management frameworks and provides a view on the potential elements of knowledge creation based on earlier literature. Chapter 4 examines social capital and its impact on knowledge creation, together with the role of shared context.

Empirical research context, approach, and methodology, together with the three cases analyzed in this research are introduced in Chapter 5, and the results and key findings from the case analysis are then presented in Chapter 6. Chapter 7 concludes the research findings, also discussing some managerial implications, research limitations and suggestions for further research.

2 Nature of knowledge

Even though knowledge management as a field of science has existed for over 30 years, there is no universal and common definition for either knowledge or knowledge management (Heisig 2009, 13; Handzig 2017, 7). In their popular book “Working knowledge” (according to Researchgate.net, the book had been cited 8004 times by March 26, 2020), Davenport and Prusak define knowledge as something people use for evaluating and incorporating new experiences and information. They state that it consists of a mix of “framed experience, values, contextual information and expert insight”, and that creating and applying it requires human activity. In organizations, knowledge exists in the form of for example documents but also as organizational processes, routines, and practices. (Davenport and Prusak 1998, 5).

In knowledge management literature, knowledge is often described to be constantly evolving and dynamic rather than static and unchanged. Knowledge can only exist when it is given a context, making it highly dependent on time and space. This means that knowledge at one moment in time within a certain context is not the same as at some other moment and in some other context. Knowledge is created in the interaction between different actors (either human actors or between human and non-human actors) and it continuously forms through the interpretations made by individuals. Knowledge accumulates and changes within these interactions. (Spender 1996, 47; Cook & Brown 1999; Nonaka et al. 2000, 7).

Understanding how (and to what extent) knowledge can be managed also requires understanding the knowledge itself. The nature of knowledge has also been widely examined and various categorizations have been created based on its different characteristics. Next, some of these categorizations and characteristics are discussed to form an understanding on how knowledge can be viewed.

2.1 Characteristics of knowledge

Knowledge exists in organizations in many forms, and the different categories and characteristics of knowledge described in knowledge management literature can be considered as reflections of its dynamic and context-specific nature. Organizational capability of knowledge creation varies between organizations and is not dependent

on the static “stock of knowledge” (Nonaka et al. 2000, 6) but understanding the various characteristics of knowledge in organizations may still help identifying possibilities for facilitating knowledge creation, especially when it comes to strategically meaningful knowledge assets (Teece 1998, 63).

Knowledge is most often categorized into the categories of tacit (implicit) and explicit knowledge, as well as individual and collective knowledge (Heisig 2009, 8). These form two dimensions, explicit/tacit and individual/collective, and are often referred to as the four most relevant categories of knowledge (Kogut & Zander 1992; Nahapiet & Ghoshal 1998; Nonaka et al. 2000). Nahapiet & Ghoshal also suggest that all intellectual capital of an organization can be described through these four categories (1998, 246-247).

The explicit/tacit dimension of knowledge is often referred to as the “epistemological dimension”, as it discusses the essence of knowledge, whereas the individual/collective dimension is known as the “ontological dimension”, as it concerns the structural and relational view of knowledge (Nonaka 1994, Lam 2000). Next section will describe each of these four “main” categories (two dimensions) and how they have been discussed in knowledge management literature.

2.1.1 Explicit/tacit dimension of knowledge

Explicit (also sometimes codified) knowledge has been described as “knowing about” (Grant 1996, 111) or “knowing what something means” (Kogut & Zander 1992, 386). What is common to these definitions is that when in explicit format, knowledge is codified and easy to be transferred. It can exist in both physical or digital format, such as blueprints, formulas, or computer code. (Kogut & Zander 1992; Nonaka 1994, 16; Grant 1996; Teece 1998, 63; Nonaka et al, 2000, 8). If not put in a context, explicit knowledge can be practically considered as “information” (Nonaka 1994, 16; Nonaka et al, 2000, 8).

Tacit knowledge (also sometimes implicit) is usually defined as “knowing how” (Grant 1996, 111; Teece 1998, 63) or “know-how, knowing how to do something” (Kogut & Zander 1992, 386). It is seen to be based on personal intuition and the observation that people cannot express all that they know (Polanyi 1958/1962; Teece 1998, 63). As it is in implicit format, it is not easily transferrable (Grant 1996,

111; Teece 1998, 63). Master-apprentice co-operation or simply other face-to-face interaction (mainly with physical dimension) is mentioned to be a suitable approach for transferring tacit knowledge, as this setup includes the possibility to “show in practice” and to have clarifying discussions that support sensemaking and learning (Nonaka 1994, 18-20; Teece 1998, 63-64).

Explicit and tacit categories are continuously interacting with each other. Explicit knowledge is used and applied with the help of tacit knowledge (for example in making decisions), and tacit knowledge is (to the extent that is possible) expressed through action within organizations. Knowledge evolves through interaction between these categories. (Nonaka 1994, 18-20; Spender 1996, 50; Nonaka et al. 2000, 8).

What distinguishes explicit and tacit categories of knowledge is not always self-evident in knowledge management literature. The characteristics connected with tacit knowledge vary from underlying knowledge that cannot be articulated, expressed, or observed, to tacit or implicit knowledge that can be expressed and observed through interaction (Polanyi 1958/1962; Nonaka 1994). For explicit knowledge, characteristics such as transferability and materiality are used, and it is always considered as tangible (Kogut & Zander 1992; Nonaka 1994, 16; Grant 1996; Teece 1998, 63; Nonaka et al, 2000, 8).

The difference between definitions of explicit knowledge, which is tangible and transferable, and information, which can be stored as it is in explicit format, has also been challenged. For example Rowley (2007, 178), based on an extensive literature review of textbooks in the fields of knowledge revolution, information systems and knowledge management, argues that “The distinction between definitions of information as data processed to be meaningful, valuable and appropriate for a specific purpose, and definitions of knowledge and ‘actionable information’ overlap and need further investigation. If knowledge is a property of the human mind, with the potential for action, explicit knowledge cannot be any more or less than information”.

Rowley’s arguments are based on the observation that information is always modified or structured through human action. However, even though the human

action would have impacted on how information has been formed, this viewpoint does not consider the human action linked to using the information. Whereas tacit knowledge is embedded within individuals, it also has a role in converting information into explicit knowledge, as it is steering the individual's process of interpreting the information. Information without human interpretation is purely information. It is only the human interaction that transforms information into knowledge and in this sense, knowledge can never be considered as an object. (Nonaka 1994; Grundstein 2013).

2.1.2 Individual/collective dimension of knowledge

Knowledge is also often categorized into individual knowledge and collective (or social/organizational/group) knowledge (Heisig 2009, 8). In principle, these knowledge categories can be described rather simply: individual knowledge is the knowledge possessed and practiced by the individual, whereas collective knowledge can be seen to be the knowledge possessed and practiced by a group (Nonaka 1994, 17; Cook & Brown, 1999).

Individual knowledge can exist in both explicit and tacit format. When in explicit format, it consists of facts, concepts and frameworks and can easily be stored and retrieved (Spender 1996, 50-51). Tacit individual knowledge can be in many forms, and it is visible for example when people exercise their skills (such as riding a bike). (Polanyi 1958/1962; Spender 1996, 50-51). As it is in tacit format, sharing it properly is difficult (Nonaka 1994, 16).

Collective knowledge (also sometimes group/social knowledge) can also be identified in both explicit and tacit format. Collective explicit (objectified, codified) knowledge is something that the organization tends to find extremely useful, as it can be shared and leveraged rather easily throughout the whole organization. Collective tacit knowledge is based on experience, and it is visible in organizational interaction, such as routines. This tacit "shared body of knowledge" can be considered as the most secure and strategically significant form of knowledge. (Spender 1996, 50-52; Nonaka & Von Krogh 2009, 636).

"Collective" as a term appears in various formats in knowledge management literature. Some researchers (e.g., Nonaka et al. 2000) use the word "collective" to

describe a group-level knowledge-related interaction as the other dimension of individual-level knowledge-related interaction. This kind of social interaction takes place “beyond individuals” and it can happen across boundaries (Nonaka 1994, 17). Some other researchers (e.g., Spender 1996) use “collective” to describe group-level tacit knowledge, whereas knowledge in groups is simply “group knowledge”. Kogut & Zander (1992) also make a distinction between collective knowledge on the levels of a group, an organization, or a network. In this study, the term “collective” knowledge is used as the other dimension together with “individual” knowledge, including both collective explicit and collective tacit knowledge (Nonaka 1994).

The four categories of explicit, tacit, individual and collective knowledge are often described as “four main categories of knowledge”. However, many researchers also describe the relationships between these categories of knowledge as somewhat dynamic and fluid, as knowledge continuously evolves (Cook & Brown 1999; Nonaka et al. 2000; Nonaka & Von Krogh 2009). Besides the four main categories, knowledge has also been categorized based on some of its other characteristics. Next section discusses these categorizations and how they describe the nature of knowledge.

2.1.3 Other categorizations of knowledge

In organizational context, knowledge can also be looked at from other “dimensions” or categories than explicit-tacit and individual-collective. This section introduces five other categorizations described in knowledge management literature: 1) Positive/negative knowledge (Teece 1998); 2) Knowledge that is observable/non-observable-in-use (Teece 1998); 3) Systemic/componential knowledge (Spender 1996); 4) Autonomous/systematic knowledge (Teece 1998), and 5) Embrained/ embodied/encultured/embedded/encoded knowledge (Blackler 1995). What makes each of these categorizations interesting from the viewpoint of this study is that they discuss such aspects of knowledge that are not directly covered by the four main categories described in the previous section.

Positive/Negative knowledge

As one of the additional knowledge categorizations, Teece (1998, 64) mentions a categorization into positive and negative knowledge. Positive knowledge is the

knowledge linked to such discoveries that may for example lead to innovations or business success, and organizations tend to willingly share this knowledge. Negative knowledge, however, is linked to threats and failures rather than successes, and not that often highlighted within organizations. Organization's capability development would still benefit from sharing both the opportunity-related, positive knowledge and threat- and failure-related, negative knowledge (such as areas of potential risks and vulnerabilities) as both aspects support new knowledge creation. (Teece, 1998, 64)

Negative knowledge and especially the potential cognitive biases leading to the challenges of identifying and sharing negative knowledge have been widely researched and discussed, and the underlying reasons for these challenges from both individual and organizational perspectives have been examined. Based on these findings, individuals have tendencies of ignoring negative knowledge for various reasons (Parviainen & Eriksson 2006; Dunning 2011), and organizational cultures impact on collective willingness of sharing negative knowledge (Serenko & Bontis 2016).

Knowledge that is observable/non-observable in use

Teece (1998, 64) also mentions that knowledge can be categorized as observable or non-observable when in use. As an example of observable knowledge, they mention that many technological devices, such as scanners, printers or microprocessors include knowledge that can be "reverse engineered" when the actual device is available. On the other hand, they see that process technology is largely non-observable when in use, or at least more difficult to be captured. (Teece 1998, 64).

This perspective can be considered to include the assumption of human interaction needed to form knowledge (discussed in the previous section), as it simply states that there is "knowledge" embedded into material objects, and that the existence of this knowledge requires it to be recognized by a human, independent of its observability, before any conclusions can be made out of this "knowledge". How Teece (1998, 64) explains this is that not knowing how a certain object (such as a machine) has been built by first observing how it operates and then making

assumptions on its construction can be one source of knowledge, but finding out how it is constructed would significantly increase this knowledge. Even though some of the technologies (such as computer code) do include capability for performing “individual actions”, this kind of action is not considered as action related to knowledge, as it does not include human activity (Robey et al. 2013, 385).

Systemic/componential knowledge

Spender (1996) brings up another categorization of knowledge: systemic knowledge vs. componential knowledge. Componential knowledge means those private-knowledge types of components that – if viewed separately – may appear disparate and incommensurate but when involved in interaction with other components are forming a system, and a basis for systemic knowledge. For example, skills of an individual can become part of organizational routines (“institutionalized”), and thereby become part of systemic knowledge. Systemic knowledge, on its behalf, is an understanding of how the entity works, and for example simulations are often used as a tool used for gaining this kind of understanding. (Spender 1996, 58).

Autonomous/systematic knowledge

Teece (1998, 64) also approaches knowledge from componential vs. systematic perspective but with a slightly different intention. They mention that a single component or an object itself can be a source for either autonomous or systematic knowledge. When a component is changed or replaced, it may or may not impact the rest of the system. In a case of autonomous knowledge, there is no impact but when the knowledge contained by the component is systematic, the changes will also require changes elsewhere in the system. (Teece 1998, 64).

Embrained/embodied/encultured/embedded/encoded knowledge

Looking at knowledge in organizations from a holistic perspective, Blackler (1995) has summarized the knowledge types in five categories that they mention to be based on initial categories first suggested by Collins in 1993. First of these categories, embrained knowledge, is individual and tacit, and originates from using conceptual skills and cognitive abilities. It is largely linked to the concept of learning and the ability to understand connections between knowledge originating from various sources. When knowledge is embodied, it has been constructed through

physical experience obtained through interaction between individuals or for example between an individual person and technology, and it can be in both explicit and tacit format. Encultured knowledge, on its behalf, involves social transformation of knowledge, leading to shared understandings (and knowledge being collective instead of individual); Blackler also compares encultured knowledge with Nonaka's views on how knowledge is created as a "process of achieving shared understandings". Embedded knowledge lies within the organization's collective systems and routines, and it is manifested through relationships between people but also within the non-human elements of the organization (such as technological systems). Finally, Blackler mentions the encoded knowledge that includes the documented knowledge, symbols, and signs in both physical and electronical (digital) format and that is in explicit format. (Blackler 1995, 1023-1026, 1033).

Blackler also states that there is a relationship between the embodied knowledge expressed via action-oriented skills and the encoded knowledge, which in the case of computer systems can be seen to either complement or replace these action-oriented skills when these systems conduct certain actions on behalf of people (1995, 1031-1032). This is also linked to the observable/non-observable knowledge mentioned by Teece (1998, 64) who says that activities conducted by technology may not be fully observable and understandable, especially if the people trying to analyze these activities cannot obtain knowledge on how the technology itself has been constructed. On the other hand, considering Rowley's (2007) observations on information requiring human interpretation to become knowledge, it can be argued that any knowledge embedded into computer-based systems, including for example automated processes or machine learning algorithms, is not actually knowledge but rather a reflection of human activities based on knowledge.

A distinct field of organizational and information systems research has been emerged around the socio-technical and sociomaterial aspects of knowledge and learning. This research aims at understanding the interaction between human and non-human (material) actors, suggesting that socio-technical aspects or sociomateriality should be considered in all organizational research, as these actors are continuously interacting and impacting each other. These fields of research also consider that knowledge is based social interaction, and they mostly maintain the

distinction between the material and social worlds based on this assumption, meaning that they do not consider material objects as such to “contain” knowledge. (Orlikowski 2007; Leonardi & Barley 2008; Robey et al. 2013).

2.1.4 Summary of different knowledge categorizations

In addition to the various categories of knowledge listed in the previous sections, there are many other categorizations available in knowledge management literature and many other ways to look at the different characteristics of knowledge. To further explain the characteristics of knowledge, a summary of the categories described in this chapter can be found in Table 2. The table also shows the connection between the other categories and the four main categories (Nonaka 1994) when explicitly mentioned by the author.

Knowledge is embodied into the whole organization and its elements, such as production equipment and information systems, as these are designed and built using knowledge, and the patterns taking place between the people, technologies and techniques are unique for each organization (Grant 1996, 112; Bhatt 2001, 70). However, these material objects cannot be considered as knowledge unless human interaction and interpretations are involved. (Teece 1998; Robey et al. 2013).

As Nonaka et al (2000, 8) state: “Knowledge creation means renewing one’s existing context and knowledge through the continuous interaction with others, either other individuals or environment.” This means knowledge is impacted by and affects everything on an ongoing basis. While this section builds an initial background for understanding the multifaceted nature of knowledge, next section will explain how dynamic nature of knowledge has been approached in knowledge management literature.

Table 2. Summary of different categorizations of knowledge.

			Nonaka 1994			
Source	**Knowledge category**	**Description**	**Explicit**	**Tacit**	**Individual**	**Collective**
Spender 1996	**Systemic**	Knowledge on how an entity works				
	Componential	Knowledge on and within an individual component				
Teece 1998	**Positive**	Knowledge linked to innovations and business success				
	Negative	Knowledge linked to threats and failures				
	Observable	Knowledge that can be obtained by observing a process or technology				
	Non-observable	Knowledge that cannot be obtained through observations				
	Autonomous	Individual component's knowledge impacts the whole system				
	Systematic	Knowledge in the component is separate from the system				
Blackler 1995	**Embrained**	Knowledge that has been created using conceptual skills and cognitive abilities (learning)		X	X	
	Embodied	Knowledge constructed through physical experience	X	X		
	Encultured	Knowledge in a form of shared understanding created through social transformation	X	X		X
	Embedded	Knowledge within organizational systems and routines, manifested through relationships, processes and technologies		X		X
	Encoded	Knowledge that is documented	X			

2.2 Dynamic nature of knowledge

Even though suggestions have been made by some researchers on combining various characteristics and categorizations of knowledge into even more simplified frameworks (e.g., Lam 2000), many researchers consider that there are challenges in making such simplifications. For example Nonaka (1994) highlights the continuous interaction between different four categories of knowledge, and Blackler (1995, 1032) emphasizes that their five categories of knowledge cannot be viewed as separate from one another, as knowledge is "multifaceted and complex". Regarding the four main categories of knowledge, explicit, tacit, individual, and

collective, it is widely agreed that continuous evolvement of knowledge takes place between these dimensions (Kogut & Zander 1992; Spender 1996; Cook & Brown 1999, Nonaka et al 2000).

One of the most popular approaches to presenting knowledge interaction between the epistemological and ontological dimensions is Nonaka's "knowledge spiral" (Nonaka 1991/2007; Nonaka 1994, 18-20; Nonaka et al. 2000, Nonaka & Von Krogh 2009). Next section will explain this approach, called the SECI process/model, and the following section will address how it has been impacting some of the other pursuits of understanding knowledge.

2.2.1 Nonaka's SECI model

SECI model, first introduced by Nonaka in 1990's, is based on the idea that understanding knowledge conversion and knowledge creation starts by recognizing that the four categories of knowledge are mutually complementary, and that it is often not possible to make a clear distinction between the explicit and tacit categories of knowledge (Nonaka & Von Krogh 2009, 638). Knowledge conversion involves all types of knowledge assets within an organization (Nonaka 1994; Nonaka et al. 2000; Nonaka & Von Krogh 2009, 643). The dynamic conversion of knowledge takes place continuously between explicit and tacit knowledge in the form of an endless spiral. (Nonaka 1991/2007; Nonaka 1994, 18-20; Nonaka & Takeuchi 1995; Nonaka et al 2000; Takeuchi & Nonaka 2002; Nonaka & Von Krogh 2009; see also Figure 3).

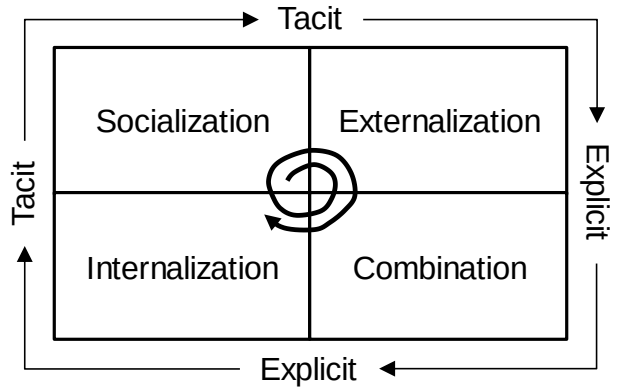


Figure 3. SECI model for knowledge conversion (Nonaka et al. 2000, 9-12).

Because knowledge evolves as an endless spiral, the process cannot be described as a traditional “process” (input-function-output). Instead, the spiral utilizes inputs all the time and as a result, knowledge continuously evolves. The spiral itself takes the knowledge through four different modes: Socialization, Externalization, Combination, and Internalization, first letters of which form the name of the model, “SECI”. The elements of the SECI model all have an important role in the evolution of knowledge. (Nonaka et al. 2000, 12).

Socialization means evolving tacit knowledge through shared experience that enables understanding of the thinking processes of knowledge creation participants. This assumes interaction between individuals and does not necessarily include any articulated (explicit) knowledge such as language or even physical motion/gestures. (Nonaka 1994; Nonaka et al. 2000)

Externalization happens when the expressible elements of tacit knowledge are materializing towards explicit knowledge. Tacit knowledge is needed for articulation so that knowledge can become explicit and transferrable. This happens through various social processes of sharing and transferring knowledge. (Nonaka 1994; Grant 1996; Teece 1998; Nonaka et al. 2000). According to Nonaka & Von Krogh, knowledge always contains a “capacity to act” and as explicit knowledge always “lags behind” from what the organization and individuals possess in the form of tacit knowledge, externalization is also needed to improve explicit knowledge (2009, 642-643).

Combination requires reconfiguring existing explicit knowledge; these activities of “sorting, adding, recategorizing and recontextualizing explicit knowledge can lead to new knowledge” (Nonaka 1994, 19). Combined knowledge may manifest for example in the form of a concept, blueprint or decision (Takeuchi & Nonaka 2002).

Internalization of knowledge has been described by Nonaka & Von Krogh as an “individual, psychological process” (2009, 642), and it means that knowledge becomes part of an individual’s tacit knowledge “in a form of shared mental models or technical know-how” (Nonaka et al. 2000, 10). Internalized knowledge is thereby “embodied” (Nonaka et al. 2000).

SECI process is not a linear process, and all four main categories of knowledge (explicit, tacit, individual, and collective) continue to exist and evolve throughout the spiral of knowledge conversion. Due to its dynamic nature, knowledge accumulates and changes continuously, and cannot be reviewed as static. (Nonaka 1994; Nonaka et al. 2000; Takeuchi & Nonaka 2002).

Knowledge conversion taking place through SECI process is at the core of knowledge creation, and knowledge creation becomes organizational level knowledge creation, when all its four modes are “organizationally” managed as a continuum. This assumes what Nonaka calls “triggers”: these are organizational activities, such as forming a team (to promote socialization), facilitating a dialogue (to support externalization), creating concepts (for combination purposes), or experimenting with new solutions (leading to internalization of knowledge). When tacit knowledge in individuals is “mobilized” through this spiral, the knowledge converted through the four modes eventually becomes collective on group, organizational or even interorganizational level. The phenomenon of organizational knowledge creation is described in Figure 4. (Nonaka 1994, 20)

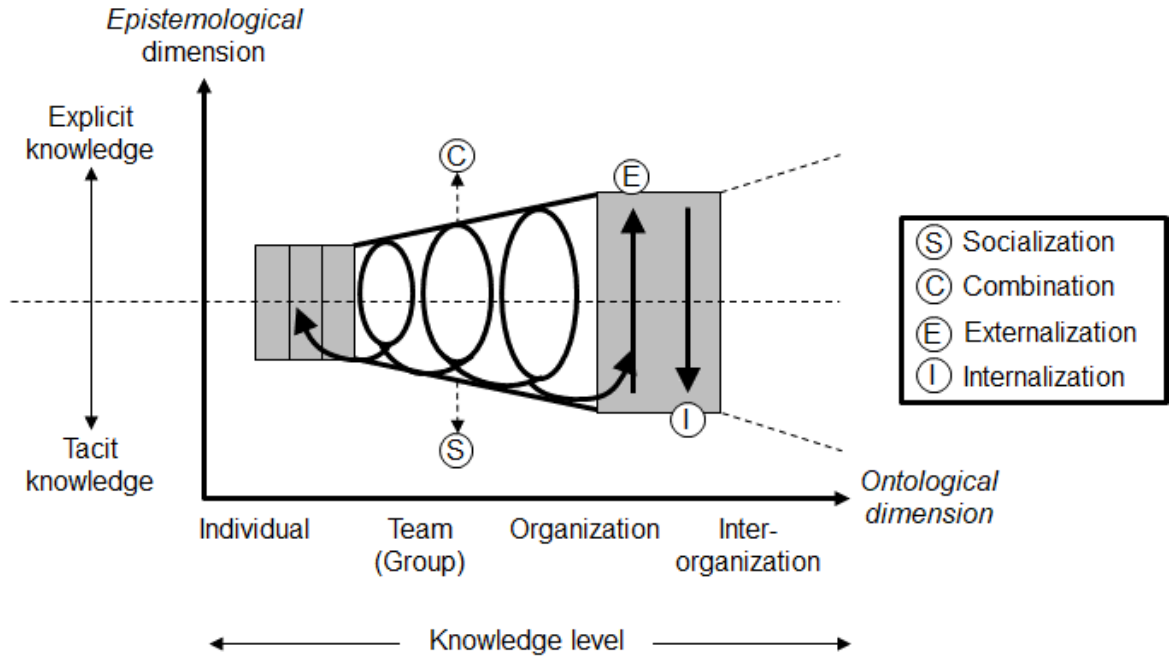


Figure 4. Spiral of organizational knowledge creation (Nonaka 1994, 20).

Nonaka, together with Takeuchi further emphasize that knowledge is most useful in its explicit format, as this enables it to be leveraged also by the rest of the

organization or by a wider audience. They see that socialization and combination are mainly related to intra-organizational knowledge (or what they call “sympathetic” knowledge), while conceptualization (taking place as part of externalization) helps leverage the created knowledge to wider audience. (Takeuchi & Nonaka 2002, 156-158)

Nonaka has been developing their work on the SECI model throughout the years, and whereas the first versions discussed mainly knowledge creation to take place in the minds of individuals or between two or more individuals in human-to-human interaction (Nonaka 1991/2007, Nonaka 1994), the later publications discuss knowledge creation as social interaction between individuals or individuals and their environment (Nonaka et al. 2000; Nonaka & Von Krogh 2009).

2.2.2 SECI model and knowing

Some potential issues that have been raised regarding the SECI process/model include the somewhat conceptual basis of knowledge conversion (especially the nature and essence of tacit and explicit dimensions of knowledge, such as how to differentiate extremely explicit knowledge and pure information/data) as well as the potential outcomes of knowledge conversion. Nonaka, together with Von Krogh, discuss this critique and – regarding the first issue – state that explicit/tacit categorization is indeed a conceptual one and mainly used for modeling a phenomenon of knowledge conversion that in reality would be much more complex. Regarding the latter issue, they admit that the nature of outcomes from knowledge conversion have not been discussed enough, and that more research is needed. (Nonaka & Von Krogh 2009).

What comes to the outcomes of knowledge conversion, both Blackler (1995) as well as Cook & Brown (1998) consider that Nonaka keeps the possession and conversion of knowledge separate from practicing of knowledge, and thereby also separates knowledge conversion from the concept of learning (which also happens through practice, including social practice). With this, they refer to the outcomes of knowledge conversion, declaring that “practicing knowledge” is an integral part of the overall knowledge creation process. Cook & Brown specifically point out that SECI model does not clearly state any action of “knowing”, even though it is both deriving from as well as contributing to the continuously evolving body of knowledge

on both the individual and collective levels. This knowing, together with tacit knowledge, is essential for all practice, also for applying explicit knowledge. (Cook & Brown 1999, 394).

Blackler (1995), approaches the potential concern of “mixing” knowledge and learning with the help of activity theory. They see that, besides the socially constructed understanding that is described as learning, also knowledge (deriving from body of knowledge) is actively present in organizational activity systems in the form of “knowing”, and is also impacting social interaction. They explain that this is a natural way to maintain the perceived distinction between knowledge and learning without ignoring the relationship between knowledge and action. Blackler describes knowing as a phenomenon that is 1) mediated, as it is continuously manifested in language, technology, collaboration and control; 2) situated, as it can be considered to be located “in time and space and specific to particular contexts”; 3) provisional, as it is both constructed and evolving; 4) pragmatic, as it has a purpose and object, and 5) contested, as it is not evenly distributed and it requires effort (Blackler 1995, 1039).

Building on SECI model of knowledge conversion (Nonaka 1994), Cook & Brown (1999) propose that the four main categories of knowledge should be used from conceptual perspective, as each of these types of knowledge, when applied in practice, have a unique functionality. They also state that the two dimensions/four categories are most suitable for describing the knowledge that is possessed (as body of knowledge) and thereby rather static, hence these dimensions can be seen to describe an “epistemology of possession”. On the other hand, when knowledge becomes part of action, it becomes knowing – a phenomenon they describe as “dynamic, concrete and relational”. This is what they call “epistemology of practice”, as it involves action and especially interaction between the body of knowledge and the situational context. (Cook & Brown 1999, 383-388, see also Figure 5).

Cook & Brown further explain that knowing, or epistemology of practice, is involved in situations where knowledge is either used in action or where knowledge is part of action. Explicit knowledge could be simplified as “knowing what” and tacit knowledge as “knowing how”, and the role of explicit knowledge in those situations would be to help gaining the tacit knowledge (e.g., one knows “in theory” and applies

this knowledge in practice) and the role of tacit knowledge is to help gain explicit knowledge (by doing something, one gains knowledge they can also explicitly express). This action also creates new knowledge. (Cook & Brown 1999).

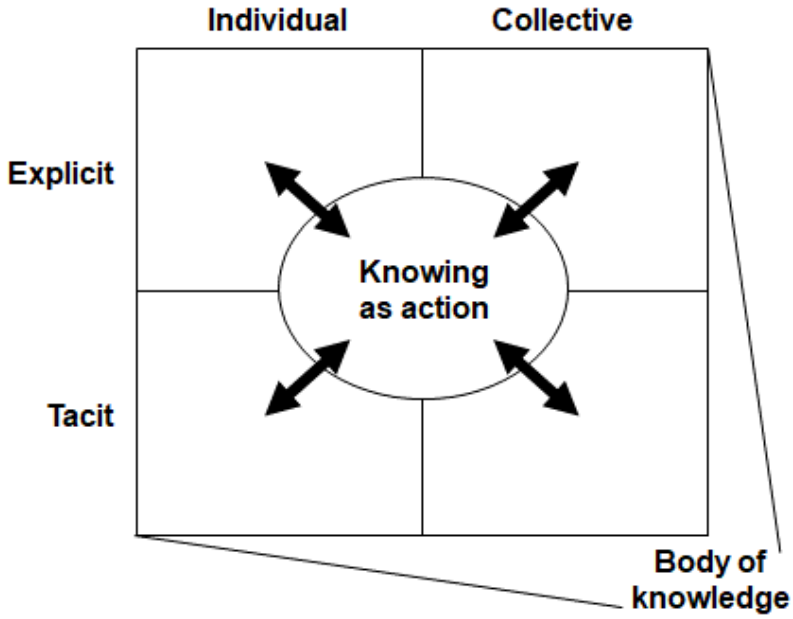


Figure 5. Adding knowing to knowledge (adapted from Cook & Brown 1999, 393).

While Nonaka's earlier work (e.g., Nonaka 1994; Nonaka et al. 2000) highlights the role of tacit knowledge in knowledge conversion, Nonaka & Von Krogh also align with the views of Cook & Brown (1999) when they admit that it is not always the tacit knowledge/knowing alone that generates action, and that also explicit knowledge may inspire action on individual or collective level. They also admit that the original organizational knowledge creation theory and the knowledge conversion model do not discuss the role of social practices and action, as this viewpoint has been developing only after the knowledge conversion theory was first introduced. To explain the conceptual differences between the theory of organizational knowledge creation and the theories of knowing and social practices, Nonaka & Von Krogh remind that the goal of the first one is to discuss how new knowledge in the organization is created, whereas the latter strives to explain "how organizations conserve tacit knowledge through social practices". (Nonaka & Von Krogh 2009, 645-646).

The constructive discussion between different researchers has aided in forming an understanding of what knowledge is, and especially how it exists. SECI model and

the related process of organizational knowledge creation describe how knowledge continuously evolves through the four main categories (explicit, tacit, individual, and collective). In their 1994 work, Nonaka actually states that SECI model aims at addressing the challenges they have come across with when viewing the concepts of organizational learning: “Theories of organizational learning do not address the critical notion of externalization, and have paid little attention to the importance of socialization even though there has been an accumulation of research on "modeling" behaviour in learning psychology” (Nonaka 1994, 19). What has originally been Nonaka’s work aiming at expanding the concept of learning, has led to further work by for example Blackler (1995) and Cook & Brown (1999), aiming at bridging the concepts of knowledge, knowledge conversion and learning with the help of “knowing”, and this work has been further considered by Nonaka & Von Krogh (2009) as an addition to Nonaka’s earlier work.

2.3 Key observations regarding nature of knowledge

Based on knowledge management literature, knowledge can be viewed from many angles. Even though criteria and characterization exist that help distinguish different formats of knowledge from each other, knowledge itself can exist in many formats simultaneously. Knowledge is constantly evolving, as it is constructed and formed through social interaction, always depending on time, place, and wider context, and always subject to individual interpretations. (Nonaka 1994; Blackler 1995; Spender 1996; Cook & Brown 1999; Nonaka et al. 2000)

When knowledge is converting through its different formats, also new knowledge is created. Knowledge creation involves continuous interaction between body of knowledge and knowing, as well as between the four main categories of knowledge. SECI model describes the conversion of knowledge between its different formats, and as knowledge is continuously evolving, also SECI takes place on both individual and collective levels and between explicit and tacit modes simultaneously and as a continuum. (Cook & Brown 1999; Nonaka et al. 2000; Nonaka & Von Krogh 2009). While SECI model and knowing describe the continuous evolvement of knowledge and thereby also how knowledge is created, the next Chapter 3 takes a further look at how knowledge creation itself has been viewed in previous knowledge management literature.

3 Knowledge creation

The various characteristics and the dynamic nature knowledge discussed in Chapter 2 show how multifaceted knowledge can be and how differently it can be viewed. Based on the SECI model introduced in section 2.2.1, new knowledge is continuously being created through knowledge conversion, and it is created even without intentional supporting or facilitation activities (Nonaka 1994; Nonaka et al. 2000; Nonaka & Von Krogh 2009).

From knowledge management perspective, organization's competitive advantage is highly dependent on its knowledge assets and how they are deployed and used (Spender 1996; Teece 1998; Grant 1999; Nonaka et al. 2000; Bhatt 2001). This knowledge and knowing capability form organization's intellectual capital (Nahapiet & Ghoshal 1998, 249). To increase their intellectual capital and improve their competitive advantage, organizations can apply various knowledge management activities and approaches (Kogut & Zander 1992; Nonaka & Takeuchi 1995; Grant 1996; Spender 1996). This chapter derives from previous literature to discuss knowledge creation as part of organizational knowledge management processes.

3.1 Knowledge creation in knowledge management frameworks

Knowledge management has been researched from various positions: technocratic school focuses on how information or management technologies support knowledge work, economic school is interested on how knowledge and intellectual capital contribute to revenue generation, whereas behavioral school examines how managers and management can facilitate knowledge creation, sharing and usage (Earl 2001, 218). Handzig (2017) has further categorized knowledge management research being related into three contexts: knowledge enablers ("social and technical factors in enabling and facilitating knowledge processes"), knowledge processes ("processes through which knowledge is moved and modified"), and knowledge stocks ("knowledge is seen as a valuable organizational asset", bringing together "different perspectives of knowledge").

Various frameworks have been created for describing the elements of knowledge management. Based on an analysis of 160 knowledge management frameworks, Heisig (2009, 15) presents a "generic" framework describing the "three focus areas"

of knowledge management (Figure 6). In Heisig's model, knowledge is a resource utilized for and produced by business processes, inside and between organizations. Business processes ("Business focus"), which are facilitated and supported by knowledge management activities, namely create, store, share and apply ("Knowledge focus"). Enablers for successful knowledge management ("Enabler focus") include ''Company culture'', ''Organization and roles'', ''Strategy and leadership'', ''Skills and motivation'', ''Controlling (and measurement)'' and ''Information technology'', and these enablers should be addressed and measured when developing knowledge management in organizations. (Heisig 2009, 15).

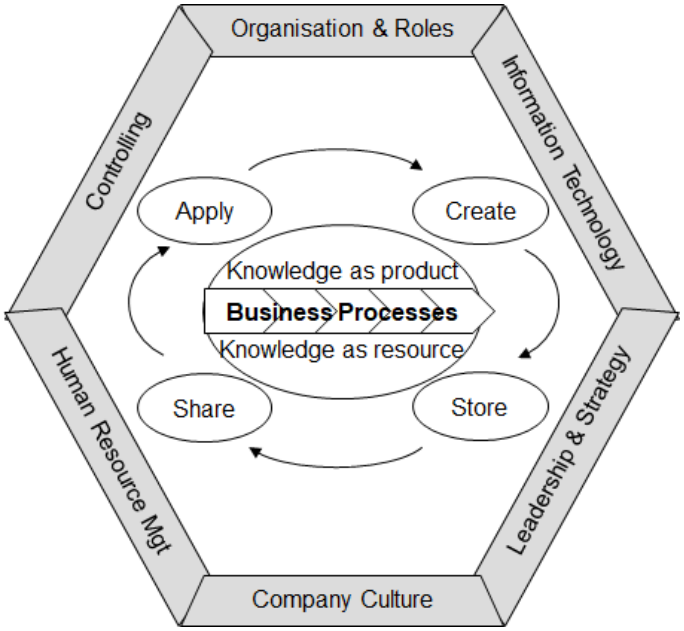


Figure 6. Heisig's GPO-WM -Framework, a three-layered model describing the focus areas of knowledge management (Heisig 2005 in Heisig 2009, 15).

Heisig states that a typical knowledge management process framework includes five activities: ''identify'', ''create'', ''store'', ''share'' and ''apply'' knowledge (Heisig 2009, 15), and that "share" is the most commonly mentioned activity. Also Hussinki et al. (2017, 1599) describe knowledge processes as "generic activities, such as the acquisition, sharing and creation of knowledge". Hence, knowledge creation is an essential part of knowledge management frameworks.

What kind of role does knowledge creation then have within knowledge management, and what does knowledge creation require? Altogether nine research

articles discussing knowledge creation were analyzed for this study with an objective to form an understanding on how knowledge creation could take place.

3.2 Elements of knowledge creation

The articles analyzed for this chapter include the work from Grant (1996), Nahapiet and Ghoshal (1998), Gupta and Govindarajan (2000), Nonaka, Toyama and Konno (2000), Bhatt (2001), Alavi & Leidner (2001), Gold, Malhotra & Segars (2001), Fong (2003), and Pinho, Rego & Pina e Cunha (2012). The articles were selected based on their different approaches on knowledge processes and especially on knowledge creation. List of the nine articles, their authors, as well as a high-level summary of how they discuss processes and how they define knowledge creation and its prerequisites/enablers can be found in Table 3.

As concluded in Chapter 2, knowledge has a dynamic and context-specific nature, and knowledge conversion takes place continuously between the four main categories of knowledge (explicit, tacit, individual, and collective), as described in the SECI model. (Nonaka 1994; Spender 1996; Cook & Brown 1999; Nonaka et al. 2000). Despite having somewhat different approaches to knowledge creation, all the reviewed articles agree that knowledge can be viewed through these four categories, and that knowledge is – at least roughly speaking – dynamic, context-specific, and evolves continuously. All the analyzed articles refer to Nonaka's work, and Grant (1996) Alavi & Leidner (2001), Fong (2003), and Pinho et al. (2012) and naturally Nonaka et al. (2000) also mention Nonaka's SECI model/knowledge conversion (e.g., Nonaka 1994) already introduced in Chapter 2 of this study. Additionally, the authors are cross-referencing on each other's work and build on each other's previous findings.

Whereas all selected articles focus on organizational knowledge, some of them also emphasize the role of the individual and their knowledge as part of the knowledge within organizations (Grant 1996; Nonaka et al. 2000; Alavi & Leidner 2001; Fong 2003). The term intellectual capital is emphasized over the term knowledge in some articles, either to highlight the organizational angle (Nahapiet & Ghoshal 1998) or knowledge as a strategic capability (Grant 1996).

Table 3. Summary of articles reviewed for Chapter 3.

Authors	Knowledge processes	Definition of knowledge creation	Enablers of knowledge creation	Title/Publication
Grant 1996	• Knowledge production: Creation of new knowledge, Acquisition of existing knowledge and Storage of knowledge • Knowledge application	• Knowledge production and application ensure organizational knowledge creation. • Firms role is to integrate knowledge possessed by each individual so that it can be applied.	• Integration and coordination mechanisms: rules, directives; sequencing; routines; group problem solving and decision making (first three drive efficiency in knowledge transfer) • Common knowledge (drives aggregation potential/capacity aka adding new knowledge to existing knowledge)	Toward a knowledge-based theory of the firm. Strategic Management Journal, Vol. 17, 109-122.
Nahapiet & Ghoshal 1998	• Knowledge creation: Knowledge exchange Knowledge combination	• Intellectual capital is created through combining knowledge, either by combining elements that have not been connected before, or developing new combinations of elements that have been connected before. • Combination can happen incrementally or radically. • Combination cannot happen without exchange.	• Three dimensions of social capital: Structural, Relational and Cognitive • Four conditions that are required for knowledge combination and exchange: Access to knowledge, Anticipation of value, Motivation, Combination capability	Social capital, intellectual capital and the organizational advantage. Academy of Management Review, Vol. 23, No. 2, 242-266.
Gupta & Govindarajan 2000	• Knowledge accumulation: Creation, Acquisition, Retention • Knowledge mobilization: Identification, Outflow, Transmission, Inflow	• Intellectual capital is created through accumulating and mobilizing knowledge. • Within accumulation, knowledge creation refers to "learning by doing", whereas acquisition means internalizing external knowledge. • Mobilization describes knowledge sharing between a sender and a receiver. • Processes of accumulation and mobilization are strongly impacted by organizational activities.	• Social ecology/social system,impacts how people interact • It is formed by culture, structure, systems, processes, people and leadership.	Knowledge management's social dimension: Lessons from Nucor Steel. MIT Sloan Management Review, Vol. 42, No. 1, 71-80.
Nonaka, Toyama & Konno 2000	• Knowledge creation process elements: SECI, Ba and knowledge assets • Process for leading knowledge creation	• Knowledge creation is about continuous transcendence of own internal and external boundaries, as knowledge is created between individuals and their environment. • It builds around SECI process, which is dynamic. • Other two process elements, ba (common context) and knowledge assets, interact through SECI process in a spiral and continuous mode.	• Leading knowledge creation: providing vision; developing and promoting the sharing of knowledge assets; building, connecting and energizing ba; promoting SECI process • Ba, meaning the shared context, is based on the conditions of autonomy, creative chaos, redundancy, requisite variety, love, care, trust & commitment.	SECI, Ba and leadership: A unified model of dynamic knowledge creation. Long Range Planning, Vol. 33, 5-34.
Bhatt 2001	• Knowledge creation • Knowledge validation • Knowledge presentation • Knowledge distribution • Knowledge application	• Knowledge creation is an ability to develop novel and useful ideas and solutions. • Knowledge creation can happen as a "fresh-start" (recommended), or by reconfiguring existing pieces of knowledge (imitation/replication/substitution), by focusing on capabilities and limiting shortcomings (with R&D), or by organizing and interpreting existing information in new light. • Knowledge management processes proceed linearly and are managed by the organization.	• Prerequisites include motivation, inspiration, experimentation and pure chance. • Enablers include culture, organizational coordination and information technology.	Knowledge management in organizations: examining the interaction between technologies, techniques, and people. Journal of Knowledge Management, Vol. 5, No. 1, 68-75.

Table 3. Summary of articles reviewed for Chapter 3.

Authors	Knowledge processes	Definition of knowledge creation	Enablers of knowledge creation	Title/Publication
Alavi & Leidner 2001	• Knowledge creation • Knowledge storage/ retrieval • Knowledge transfer • Knowledge application	• Knowledge creation is about developing new content or replacing existing content. • Knowledge creation is based on both social and collaborative processes, and individual cognitive processes, and is based on SECI Processes.	• Knowledge creation requires ba (which is interpreted as "common place or space") • Article is discussing knowledge management systems, which are seen as an enabler	Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS Quarterly, Vol. 25, No. 1, 107-136.
Gold, Malhotra & Segars 2001	• Knowledge acquisition (acquire, seek, generate, create, capture, collaborate) • Knowledge conversion (organize, integrate, combine, structure, coordinate & distribute) • Knowledge application (storage, retrieval, application, contribution, and sharing), • Knowledge protection	• Knowledge creation is part of knowledge acquisition, and it takes place in two ways: seeking and acquiring knowledge that is new for the organization, or creating new knowledge out of existing knowledge through collaboration. • Collaboration happens both between individuals and organizations, and the collaboration between individuals creates knowledge and is the basis for socialization.	• Infrastructural capabilities enable maximization of social capital, and social capital is needed for combination & exchange which enable creating new knowledge. • Infrastructural capabilities consist of Structural (norms & trust mechanisms, promoting sharing across boundaries; modular, flexible, self-organizing structures); Cultural (shared contexts; interaction and collaboration, purpose & vision, values: trust & openness; and Technological (technology enabled connections) capabilities.	Knowledge Management: An Organizational Capabilities Perspective. Journal of Management Information Systems, Vol. 18, No. 1, 185-214.
Fong 2003	• Knowledge creation in project teams: Boundary-crossing Knowledge sharing Knowledge generation Knowledge integration Collective project learning	• Knowledge creation processes in project context are "interwoven". • Boundary crossing is a prerequisite leading to knowledge sharing, knowledge generation and knowledge integration. • Collective learning is central to all three processes and can occur in individuals, within teams and between projects. • Knowledge also accumulates in the continuum of projects among participants.	• Boundary-crossing is seen crucial for the knowledge exchange and combination to happen, and it is supported by knowledge redundancy, boundary objects and mutual respect towards each other's expertise. • Other phases are facilitated for example by managerial activities, utilizing social networks and creating common objects (such as documentation)	Knowledge creation in multidisciplinary project teams: An empirical study of the processes and their dynamic interrelationships. International Journal of Project Management, Vol. 21, 479-486.
Pinho, Rego & Pina e Cunha 2012	• Knowledge acquisition • Knowledge creation • Knowledge sharing • Knowledge transfer	• Knowledge creation is taking place as an interaction, via SECI process. • Knowledge creation differs from acquisition, which is proactive "search for" knowledge, whereas creation is taking place in interaction (via SECI process) • Sharing involves tacit knowledge and transfer focuses on explicit knowledge.	• Knowledge creation has many facilitators and barriers, which the authors categorize as Technological, Socio-organizational, or Individual.	Improving knowledge management processes: A hybrid positive approach. Journal of Knowledge Management, Vol.16 No. 2, 215-242.

Level of detail for describing knowledge creation process in the selected articles depends on whether the authors discuss all knowledge management processes (Grant 1996; Gupta & Govindarajan 2000; Bhatt 2001; Alavi & Leidner 2001; Gold et al. 2001; Pinho et al. 2012), or whether they focus mainly on knowledge creation (Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003). Those authors who look at knowledge management processes as an end-to-end framework discuss knowledge acquisition and knowledge creation as the first steps, and then the rest of the process phases assume knowledge to "exist" so that it can be acted upon during those phases. Naturally, those authors who focus mainly on knowledge creation also describe the elements of knowledge creation with more detail.

The authors also place different emphasis on the organization's role in facilitating or coordinating knowledge management processes, yet all of them do see that the organization can impact these. Those authors (Grant 1996; Gupta & Govindarajan 2000; Gold et al. 2001) who emphasize the role of the organization in steering knowledge management processes consider leading knowledge management activities as one of the most important tasks of the organization, whereas those authors who mention that knowledge processes take place between individuals and groups also without an active facilitation (Nonaka et al. 2000; Alavi & Leidner 2001) also see that there are supporting activities that can be applied to enhance and facilitate these processes. The first approach seems to be in line with what Handzig describes as the "Technocratic school" and specifically its sub-school, the "Engineering school" of knowledge management focusing on processes and knowledge flows, and the second approach leans more towards the "Behavioral school" of knowledge management. (Handzig 2017, 12).

Next sections further explain how the articles listed in Table 3 describe organizational knowledge creation and what do they see as enablers/prerequisites for this to take place.

3.2.1 Acquiring knowledge vs creating knowledge

Some of the knowledge management process approaches reviewed for this study seem to treat the acquisition of existing knowledge as a separate process from the creation of new knowledge. Bringing up a concept of "knowledge production", Grant sees that organizations either acquire (existing) knowledge from outside or create

knowledge within the organization, and that both knowledge acquired into and knowledge created within the organization are stored with the help of organizational activities (1996, 112). Pinho et al (2012, 218) are seemingly following a similar pattern, as they explain that knowledge acquisition as a proactive approach for finding and organizing what they call “information/knowledge”, whereas they see knowledge creation as converting the individual level knowledge into organizational level knowledge.

Gupta & Govindarajan describe knowledge creation as “learning by doing” and knowledge acquisition as “internalization of external knowledge”. As an example of the latter, they mention that an organization can acquire technological knowledge and start using it. However, they do seem to take into consideration that adapting these technologies into the use of the organization and using them also involves other than the “internalized external knowledge”. (Gupta & Govindarajan 2000 (2000, 73, 76). Gold et al. mention a similar distinction between acquisition and creation: they see that the two ways of creating “new knowledge” include seeking and acquiring knowledge that is new to the organization (similarly to Gupta & Govindarajan’s “knowledge acquisition”), and creating new knowledge based on existing knowledge via collaboration (Gold et al. 2001, 195).

As discussed in Chapter 2, the dynamic nature of knowledge includes an assumption that it evolves continuously (Nonaka 1994; Cook & Brown 1999), and that that this evolvement takes place when knowledge is interpreted in social interaction which involves both the existing knowledge and new knowledge (Nonaka 1994; Grundstein 2013). Within the reviewed articles, Bhatt (2001) mentions that existing knowledge can be interpreted in new light as a result of collaboration, and both Nonaka et al. (2000) and Alavi & Leidner (2001) propose that existing knowledge plays a part in new knowledge creation: it can be a source for building a “common ground”, and it actually is the starting point for knowledge creation, as it is the basis for the conversion into new knowledge through the SECI model.

The approach to separate new knowledge creation and existing knowledge acquisition in the reviewed literature generates a question of the novelty of knowledge: when is knowledge considered to be “new” and when is it considered “existing”? Bhatt (2001) sees that this boils down to “new realities and meanings”

and the ability to solve existing problems or generate new innovations. Nahapiet & Ghoshal (1998, 248) state that knowledge combination can take place either as an incremental change, mainly through developing already existing knowledge, or as a more radical change, leading to an innovation.

Knowledge can be “new” to an individual or organization, but it is never completely new, as it is created through an interaction that is based on existing knowledge. Gold et al. (2001) and Fong (2003) propose that knowledge accumulates on continuous basis through socialization and interaction, and that new knowledge is emerging through this collaboration. Nonaka et al. (2000) and Alavi & Leidner (2001) also emphasize the dynamic constantly evolving nature of knowledge and endless spiral of knowledge creation.

3.2.2 Sharing knowledge to create knowledge

Even though all the analysed knowledge management process descriptions (listed in Table 3) do not explicitly bring up the dynamic nature of knowledge or non-linear nature of knowledge processes, they all bring up the continuous accumulation of knowledge. Nonaka et al (2000) and Fong (2003) discuss the meaning of knowledge sharing/transfer as a prerequisite for knowledge creation; knowledge needs to be shared/transferred so that it can act as an input for knowledge creation. Nahapiet and Ghoshal (1998) refer to this connection by stating that knowledge combination cannot happen without knowledge exchange, and they consider access to the knowledge and the parties holding it as an important pre-condition for knowledge creation.

Nonaka et al (2000) and Alavi & Leidner (2001) consider that knowledge can be shared in interaction independent on whether it is in explicit or tacit format, whereas Bhatt (2001) and Gold et al. (2001) seem to refer more to explicit knowledge when discussing knowledge sharing activities. Pinho et al. (2012) suggest that knowledge sharing would involve tacit knowledge, whereas knowledge transfer would focus on explicit knowledge and would not require human interaction.

As discussed in Chapter 2, human interaction is required to interpret transferrable information before it becomes knowledge (Nonaka 1994; Grundstein 2013). Gupta and Govindarajan (2001) seem to pay additional attention to the organization’s role

in pursuing what they call knowledge mobilization, which consists of knowledge identification (opportunities for sharing), knowledge outflow (motivating the sender to share the knowledge), knowledge transmission (channels for sharing), and knowledge inflow (motivating the receiver to accept and use the knowledge), and which is considered to be an essential part of knowledge creation together with knowledge acquisition.

3.2.3 SECI model and knowledge creation

Regarding the reviewed literature (Table 3), most authors do not introduce specific elements or process for knowledge creation itself but rather describe it as part of knowledge management processes. Among the selected authors, Alavi & Leidner (2001); Fong (2003), Pinho et al. (2012) as well as Nonaka et al. (2000) see Nonaka's (1994) SECI model and its four modes (socialization, externalization, combination, and internalization) as an essential part of knowledge creation. Fong also continues to build on the SECI model by stating that socialization and externalization phases are the same as knowledge sharing (socialization related to tacit and externalization to explicit knowledge), whereas combination can be considered knowledge integration, and internalization as collective project learning (Fong 2003, 481).

Fong's (2003) observation also sheds new light on some of the other papers. Nahapiet & Ghoshal (1998) describe knowledge combination and exchange, stating that these two activities should be reviewed as interlinked: Knowledge exchange is a prerequisite for resource combination, and thereby combination is dependent on exchange. Knowledge combination means making new combinations based on the existing (explicit and tacit) knowledge by combining knowledge that has not been connected previously, or creating new connections between already connected elements, or both. Combination can take place either as an incremental change, mainly through developing already existing knowledge, or as a more radical change, leading to an innovation. (Nahapiet & Ghoshal 1998, 248).

As the (knowledge) resources for exchange and combination are usually held by different parties, knowledge exchange of both tacit and explicit knowledge is needed for knowledge combination, and this requires social interaction (Nahapiet & Ghoshal, 1998). Using Fong's (2003) logic to compare Nahapiet & Ghoshal's

knowledge creation with Nonaka's et al. model, exchange (sharing) mainly takes place through socialization and externalization, whereas combination/integration is closer to combination and internalization within Nonaka's SECI model (Nonaka 1994; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003). Figure 7 describes the logical alignment between these concepts.

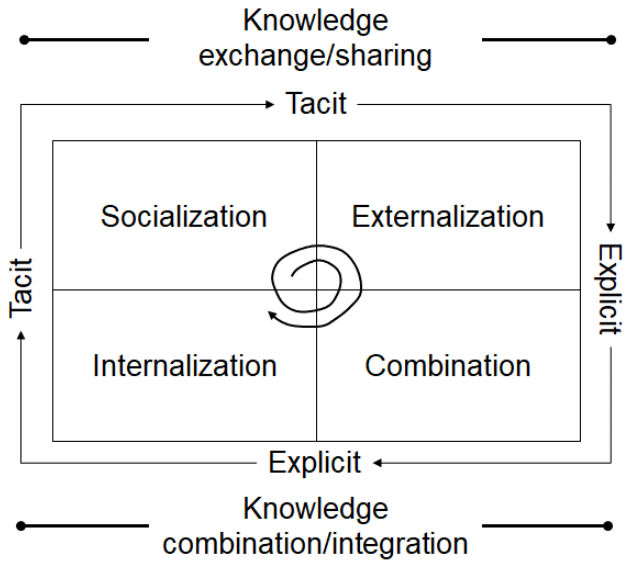


Figure 7. Alignment between three knowledge creation models.

(SECI model (Nonaka 1994; Nonaka et al. 2000), knowledge exchange and combination (Nahapiet & Ghoshal 1998) and knowledge sharing and integration (Fong 2003) as understood by the researcher).

Regarding SECI model, both Alavi & Leidner (2001) and Pinho et al. (2012) see that it explicitly describes knowledge creation, and consider knowledge sharing as a separate activity. On their behalf, Grant 1996, Gupta & Govindarajan (2000) and Gold et al. (2001) who do not bring up SECI model in their work, describe acquisition, creation, and sharing (or application/mobilization) as a continuum.

Nonaka et al. (2000) consider SECI as the core of knowledge creation, being the self-driven phenomenon that converts and develops knowledge. SECI happens in interaction with two other elements: "ba", a shared context where knowledge is created, and knowledge assets, consisting of inputs, outputs and moderator of the knowledge creating process. (Nonaka et al. 2000, 8-9).

The concept of “ba” (illustrated in Figure 8), is described by Nonaka et al. as “shared context in motion”. It is an event where individual contexts of each party interact around a shared context. As it is an event, it involves time (or temporal dimension) and location (not necessarily a physical one) where the shared context exists. Individuals involved in “ba” are inside its boundaries, but not limited by it. (Nonaka et al. 2000, 13-15)

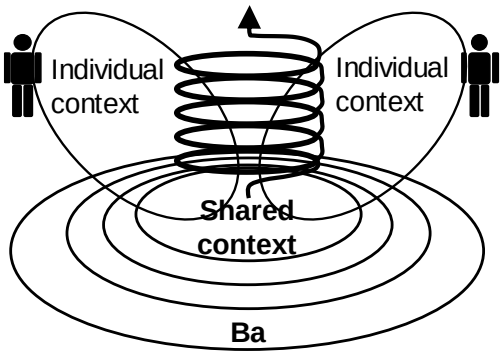


Figure 8. “Ba” as a shared context in motion (Nonaka et al, 2000, 14).

The third element of knowledge creation in Nonaka’s et al. (2000, 20) model in addition to SECI and “ba” are knowledge assets, which they describe as “acting as inputs, outputs and moderating factors of the knowledge-creating process”. They consist of four categories, two of which are based on tacit knowledge and two on explicit knowledge:

1) **Experiential knowledge assets** include “tacit knowledge that is shared through common experiences”, such as individual skills and know-how, love, trust, security, and care, as well as energy, passion and tension.
2) **Routine knowledge assets** are based on “tacit knowledge routinized and embedded in actions and practices”, including know-how in daily operations, organizational routines, and organizational culture.
3) **Conceptual knowledge assets** are based on explicit knowledge. This category includes assets such as product concepts, design, and brand equity.
4) **Systemic knowledge assets** are systemized and packaged explicit knowledge, and exist in the forms of documents, specifications, manuals, databases, patents, and licences. (Nonaka et al. 2000, 20).

According to Nonaka et al. (2000), also the knowledge assets are continuously evolving as part of the continuous SECI conversion within different levels of organizations but despite this, organizations should still map their knowledge assets. By mapping their knowledge assets, organizations would be able to recognize and support the development of knowledge as it is continuously evolving through the SECI conversion that takes place within organization's various "ba". (Nonaka et al. 2000)

3.2.5 Enablers/prerequisites for knowledge creation

Knowledge-related interaction takes place continuously even without intentional facilitation, but it can be enhanced with intentional activities (Nonaka 1994, Nonaka et al. 2000). Research reviewed for this chapter mentions several enablers, prerequisites or pre-conditions that impact organization's ability to create knowledge, as well as some intentional activities that can be applied to enhance these enablers or make the conditions more suitable for promoting knowledge creation.

Pinho et al. (2012) have collected potential barriers and facilitators for knowledge management processes via an extensive literature review. As a result, they list four elements that impact knowledge processes: 1) adjustment between IT systems and processes, and/or between IT systems/processes; 2) internal social capital; 3) external social capital; and 4) individual social/relational capital (individual-level trust and co-operation with others). (Pinho et al. 2012)

The four elements identified by Pinho et al. (2012) can be identified also to some extent in the other reviewed articles. Bhatt (2000) mentions that knowledge management consists of both technological and social systems, and Gold et al. (2001) divide knowledge management capabilities into infrastructure and processes, where infrastructure consists of both social and technical capabilities. However, the role of technology (one of the four elements identified by Pinho et al.) as an enabler of knowledge creation and knowledge management is seen as less important compared with the role of the social systems/ecology (Bhatt 2000; Gold et al. 2001; Gupta & Govindarajan 2001), and some of the articles do not mention technology at all or mention it only briefly (Grant 1996; Nahapiet & Ghoshal 1998;

Nonaka et al. 2000; Fong 2003). It should however be noted that this observation may result directly from the selection of articles for this review: besides Pinho et al. (2012), only Alavi & Leidner (2001) put a strong emphasis on the technological aspect in their article.

On the other hand, all articles bring up various viewpoints regarding the role of the social conditions/context/system in knowledge creation and knowledge management. Bhatt (2000) sees that especially culture has a strong impact on the organization's capability to create unique patterns of its people, technologies, and techniques, and Nonaka et al. (2000, 25-27) discuss five conditions that would be required for "energizing ba", the shared time and place related context for knowledge creation: 1) autonomy; 2) creative chaos; 3) requisite variety; 4) love, care, trust and commitment; and 5) redundancy. Also Grant (1996, 115) discusses the importance of "common knowledge" or knowledge overlap (referring to Nonaka's redundancy) that permits individuals to share and integrate knowledge aspects that would otherwise remain as individual.

Gold et al. (2001) mention the essential role of social capital in combination and exchange, and list certain infrastructural capabilities that help maximizing social capital. These include norms & trust mechanisms, promoting sharing across boundaries (with the help of structures), cultural aspects (such as purpose and vision, values, and shared context), and technological ties (Gold et al. 2001, 188-189). Nahapiet and Ghoshal (1998), on their behalf, have approached the entire creation of intellectual capital specifically by examining how social capital and its different dimensions facilitate knowledge exchange and creation.

When it comes to the potential enablers and prerequisites for knowledge creation, it seems that most of the reviewed literature puts a stronger emphasis on social systems/social capital related enablers and prerequisites than on technological enablers. As knowledge is accumulated through continuous social interaction (Nonaka 1994, 18-20; Spender 1996, 50; Nonaka et al. 2000, 8), the role of social capital as an enabler for this interaction and especially knowledge exchange and combination appears to be quite natural (Nahapiet & Ghoshal, 1998).

3.3 Summary of knowledge creation

Based on the literature review conducted for this study, knowledge creation can be approached from different angles: as part of a holistic knowledge management process framework and owned and steered by the organization, or as a natural phenomenon that can be intentionally enhanced with certain activities and conditions. From knowledge management viewpoint, knowledge is created in interaction, and even though the researchers are not in full agreement on what the precise mechanism for knowledge creation is, they have accepted this as part of the dynamic nature of knowledge.

As discussed in this chapter, both similarities and differences can be found when reviewing previous literature. Based on the review of the nine articles (listed in Table 3), two of the similarities seem to be prevailing:

1) Knowledge creation can be described with the help of SECI model (also describing it as acquisition/sharing and integration, or exchange and combination) (Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003).
2) Social system/social capital related enablers and prerequisites are more important enablers and prerequisites of knowledge creation than technological enablers/tools (Grant 1996; Nahapiet & Ghoshal 1998; Bhatt 2000; Nonaka et al. 2000; Gold et al. 2001; Gupta & Govindarajan 2001; Fong 2003).

Whereas SECI model is already discussed in Chapter 2, the following Chapter 4, will take a deeper look on the role of social capital in knowledge creation.

4 Social capital and knowledge creation

As discussed in Chapter 3, previous research highlights the role of social systems and especially social capital in knowledge creation. Nahapiet & Ghoshal (1998) have particularly examined the connections between social capital and intellectual capital/knowledge creation, and their starting point has been to understand, how the structural, relational, and cognitive dimensions of social capital promote the conditions of knowledge exchange and combination.

This chapter discusses the role of social capital in knowledge creation in more detail, and it builds on the approach of linking three dimensions of social capital into knowledge creation, originally introduced by Nahapiet & Ghoshal (1998). First, Nahapiet & Ghoshal's concept of three dimensions of social capital are described, followed by a discussion on how these dimensions impact knowledge exchange and combination. Finally, these viewpoints are connected to other similar findings in previous literature, especially concerning the role of shared context in knowledge creation.

4.1 Three dimensions of social capital

Organization's intellectual capital is formed through its knowledge assets (Teece 1998; Marr 2008), and in some of the models describing intellectual capital, also social capital has been separately mentioned as one of its elements (e.g., Käpylä et al. 2012; Salonius & Lönnqvist 2012; or "Social innovation capital" in McElroy 2002). On the other hand, in some intellectual capital models, social capital is not separately highlighted but can be considered as embedded. In such models, compared with the elements forming the other categories (such as human capital, relational capital, and structural capital) social capital is present in social activities and social interactions. (Ferenhof et al. 2015)

In line with the latter approach, social capital can also be considered as one of the conceptions or lenses for examining intellectual capital. This so-called relational approach emphasizes the social interaction as a basis for knowledge and focuses on understanding the role of collaboration in the development of intellectual assets (Kianto & Waajakoski 2010). The underlying thought of this approach, also called a socio-centric approach, is that the knowledge or the content is created within network ties, which themselves are one manifestation of social capital, and there is also social capital embedded within these ties (Adler & Kwon 2000).

Nahapiet & Ghoshal consider social capital mainly as a by-product of many activities and mention that it is bounded to its context (primarily to some "physical or social basis for grouping"), one example of such boundary being "the firm" (1998, 261). They describe social capital as a resource for social action and suggest that social capital impacts knowledge combination and exchange through three dimensions: structural, relational and cognitive dimension. (Nahapiet & Ghoshal 1998, 243-244).

Similar dimensions are also mentioned also in other social capital literature: Adler and Kwon (2000) discuss networks (as in Nahapiet & Ghoshal's structural dimension), shared norms (relational dimension) and shared beliefs (cognitive dimension), whereas Lesser (2000) uses structure of relationships, interpersonal dynamics within relationships, and common context and language.

Structural dimension of social capital consists of the properties of the entire system; hence, it is formed through overall patterns of connections between actors (who you reach and how), density, connectivity and hierarchy of linkages, and the organization itself. Nahapiet & Ghoshal see the structural dimension contains three important facets: 1) network ties, describing the connections between the actors in a network; 2) network configuration, characterized by the quality of these ties; and 3) appropriable organization, meaning the various uses of the network. (Nahapiet & Ghoshal 1998, 244). Among other social capital theorists, Lesser (2000) sees this dimension to describe the structure of the relationships, whereas Adler & Kwon (2000) mainly discuss the structure of networks.

Relational dimension of social capital emerges through personal relationships of individuals that have been developed over time within the organization/system. These relationships have an impact on how people behave, and how they create and leverage different assets through these bonds. Nahapiet & Ghoshal consider this dimension to consist of trust, norms, obligations, and identification. (Nahapiet & Ghoshal 1998, 244). Adler & Kwon (2000) state that the relational capital resides within shared norms, while Lesser (2000, 13-14) describes it as "interpersonal dynamics within relationships".

Cognitive dimension of social capital includes those resources that provide shared representations, interpretations, and meanings among parties. Nahapiet and Ghoshal specifically discuss shared language and codes, and shared narratives (1998, 244), whereas Lesser (2000, 13-14) talks about common context and language and Adler & Kwon (2000, 99) use the expression "shared beliefs". They see both the cognitive and relational dimension describing the amount of social capital (value) embedded within the networks, especially within network ties that are the context where the content is created (Adler & Kwon 2000, 100).

Nahapiet & Ghoshal present that an organization can develop the structural dimension of its social capital in a coordinated manner by explicitly facilitating the connections within the organization, whereas relational and cognitive dimensions are developed mainly through tacit knowledge. All the three dimensions impact each other in both positive and negative ways, and not always with a positive correlation. (Nahapiet & Ghoshal 1998, 243-245)

4.2 Impact of social capital to conditions of knowledge creation

As discussed in the previous chapters, organizational knowledge creation assumes both sharing/exchange, and combination/integration of knowledge (Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003; see also Figure 7). Grant suggests a combination of proactive steering mechanisms (rules and directives, sequencing, routines, as well as group problem solving and decision-making) to pursue the integration activities, and common knowledge (for example common language) to ensure knowledge is actually aggregated to existing knowledge and integrated as part of the organization-level operations, practices and decision-making (Grant 1996, 111, 114-115).

Nahapiet and Ghoshal (1998), in their turn, state four conditions that are required before combination and exchange can take place: 1) Access to parties for combining/exchanging intellectual capital (knowledge); 2) Anticipation of value through combining/exchanging intellectual capital; 3) Motivation to combine/exchange intellectual capital; and 4) Combination capability. All four conditions are essential for knowledge exchange and combination. (Nahapiet & Ghoshal 1998).

First condition for knowledge exchange and combination is the access to knowledge; to be able to get engaged into knowledge creation, the parties need to have an opportunity to do so, and this requires having an access to the potential sources of knowledge. In addition to the access, also the intention to get engaged into knowledge exchange and combination needs to be in place. The intention is created via two other conditions, anticipation of value and motivation. Parties need to anticipate that there will be some value arising from exchange and combination (even though at this stage the outcome would still be uncertain), and they also need to be motivated to get engaged to these activities. All these three conditions together

create the momentum for knowledge exchange and combination. (Nahapiet & Ghoshal 1998, 249).

In addition to the access to knowledge, anticipation of value, and motivation, also a fourth condition, combination capability, needs to be in place before knowledge can be exchanged and combined. Combination capability includes the ability and means to act and combine knowledge in a way that knowledge on both collective and individual level will become different compared with the previous knowledge. Without combination capability, knowledge creation cannot take place as the parties do not have any means to exchange and combine knowledge. (Nahapiet & Ghoshal 1998, 249-250).

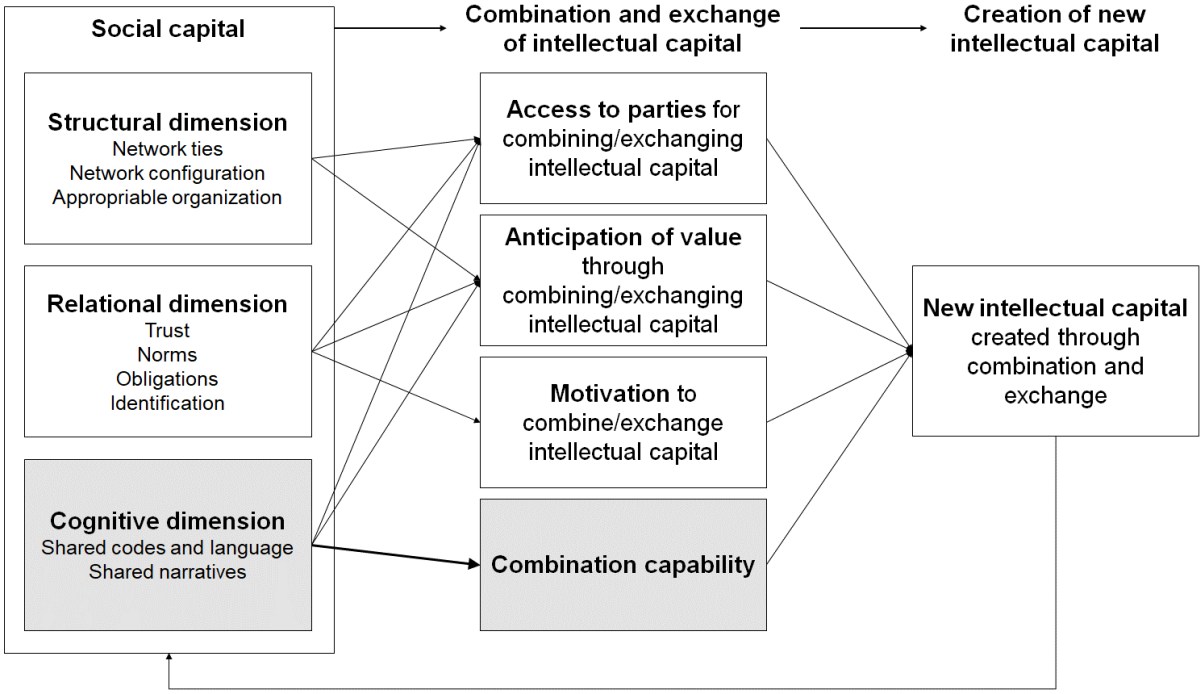


Figure 9. Social capital in the creation of intellectual capital (adapted from Nahapiet & Ghoshal 1998, 251).

Nahapiet & Ghoshal have conducted an extensive analysis of previous literature to identify causal relationships between social capital and knowledge creation. They suggest that all the facets within the structural, relational, and cognitive dimensions of social capital impact at least one of the four conditions of knowledge exchange and combination. Figure 9 includes a description of these causal relationships. (Nahapiet & Ghoshal 1998). Next, these causal relationships between each

dimension of social capital and the conditions of knowledge exchange and combination are further described, as well as discussed in the light of other previous literature.

4.2.1 Impact of structural dimension

As already mentioned, Nahapiet & Ghoshal consider structural dimension having three facets: network ties, network configuration and appropriable organization. These facets have an impact primarily on the condition of having access to parties and knowledge. Network ties represent the channels for exchange and combination, describing the “who knows who” connections. These ties have a direct impact on what one knows and the knowledge they can access. Network ties also impact on anticipation of value as well as motivation. (Nahapiet & Ghoshal 1998, 251-253, see also Figure 9).

Network configuration means the quality of these ties and the network they form, such as their density or flexibility. Organization and its appropriability reflects the relational patterns between parties; an “appropriable” organization enables the required access to knowledge. Organization’s appropriability also has an impact on access to knowledge on a larger scale, as it enables connections with other networks and organizations the parties are involved with. (Nahapiet & Ghoshal 1998, 251-253). Structural dimension also has a connection to the development of relational and cognitive dimensions of social capital. For example, strong affective ties arising from structural dimension will have an impact on the level of trust between the parties, and thereby also the motivation for sharing knowledge. (Nahapiet & Ghoshal 1998, 251-253).

Structural dimension, as well as the other two dimensions of social capital can both promote and hinder knowledge exchange and combination (Nahapiet & Ghoshal 1998). Grant (1996) and Gold et al. (2001) discuss boundaries arising from organizational structure, whereas Fong (2003) mentions boundaries between different professional disciplines and those between representatives of different organizations and between different levels of hierarchy.

Grant (1996, 117-119) sees that organizational structures and the boundaries they include can both support and hinder knowledge production. Bhatt (2000, 73)

emphasizes the need for a culture that nourishes interaction across the organization. As there is always knowledge that does not lie within the conceptual boundaries of a certain organizational entity but is still needed for that entity to fulfill its goals, the organization needs to have flexibility in structures and hierarchies at all levels of the organization but also between the organizations (Grant 1996, 120)

Organizations can support unusual patterns of connections and thereby rearrange the structural dimension of their social capital to improve conditions for knowledge combination and exchange (Nahapiet & Ghoshal, 1998). Also Grant (1996) and Gold et al (2000, 188) see that sharing across boundaries can be promoted through structures, highlighting the modularity, flexibility and fluidity in planning the organizations. Conscious collaboration supports boundary-crossing and knowledge creation between different disciplines and across all levels of organizations and between organizations (Fong 2003, 483).

4.2.2 Impact of relational dimension

Relational dimension consists of trust, norms, obligations, and identification, and these elements impact on access to parties, anticipation of value and the motivation of parties. Trust is based on the expectations of good intentions, competence, capability, reliability, and openness of the other party. It acts as a basis for an individual's willingness to share knowledge and approach the other parties, and thereby it impacts on access, anticipation of value and motivation, as there is trust that the contact is valuable. (Nahapiet & Ghoshal 1998, 254-256).

Norms, even though they are collective, are followed by individuals, and if the norms assume co-operation, they drive both access and motivation. Obligations and expectations are similar to norms but rather based on personal relationships; both are emerging through commitment and duty between the parties, affecting on both access and motivation. Identification describes a sense of togetherness or belonging between the parties but also between an individual and the group or the organization, and it affects both the anticipation of value as well as motivation. (Nahapiet & Ghoshal 1998, 254-256)

Some of the elements of relational dimension of social capital can also be identified in the literature reviewed for Chapter 3. Gold et al. (2001, 187) consider trust and

norms as part of their concept of infrastructure (particularly what they call “structural infrastructure”), which is required for knowledge management activities to take place. Gupta & Govindarajan (2000, 75-76) highlight the positive impact of norms, obligations, and expectations such as tolerance for failure, employee empowerment, or high degree of accountability, loyalty and commitment to knowledge acquisition and creation. Nonaka et al. (2000) see that fostering care, trust and commitment especially promotes knowledge socialization (which is linked to Nahapiet & Ghoshal’s knowledge exchange, see also Figure 7).

4.2.3 Impact of cognitive dimension

Nahapiet & Ghoshal state that “knowledge and meaning are always embedded in social context, both created and sustained through ongoing relationships in such collectives” (1998, 253). They describe cognitive dimension to be based on the idea of intellectual capital being mainly a “social artifact”. Even though innovation assumes different knowledge and experience (difference), there still needs to be at least some shared context for social exchange and combination to take place. They see that there are two elements of cognitive combination that are required for enabling combination capability: shared language and vocabulary/code as well as shared narratives. Regarding the three dimensions of social capital, cognitive dimension is thereby considered as the primary prerequisite for combination capability (as highlighted in Figure 9). (Nahapiet & Ghoshal 1998, 253).

Shared language and codes are also required for enabling access to parties, as they act as a tool for discussion and exchange in the first place. As they strongly affect how the parties involved in exchange and combination observe and interpret the knowledge and the process itself, they also have an impact on how the parties form their perceptions. For combination capability, this means that there needs to be at least some overlap of knowledge to facilitate both the exchange and combination of the information gained through social exchange, as otherwise it would not be possible for parties to understand each other’s perspectives and to form joint perceptions. (Nahapiet & Ghoshal 1998, 253-254)

Another element of cognitive dimension of social capital are shared narratives, which Nahapiet & Ghoshal describe to be embedded with deeper meanings than

pure information. As narratives combine information with practical experience, they can also facilitate sharing of tacit knowledge. (Nahapiet & Ghoshal 1998, 254).

Similarly to Nahapiet & Ghoshal's (1998) shared language, codes and narratives as means for increasing the common cognitive ground, Fong (2003) discusses the role of boundary objects (such as drawings, personal conversations) as tools to facilitate crossing the boundaries that exist for example between different professions. Understanding multiple viewpoints and valuing the expertise of others can help crossing organizational boundaries (Fong 2003), and to succeed, understanding various perspectives requires a common ground (Nahapiet & Ghoshal 1998).

In knowledge creation related literature reviewed for this study, the cognitive dimension and shared context receive significant attention: for example Blackler (1995) calls this encultured knowledge and sees it as the enabler for social interaction whereas Takeuchi & Nonaka (2002) as well as Grant (1996) see the common knowledge as an important enabler of socialization and combination. Cognitive dimension and shared context are required to be able to combine the knowledge of different parties. However, as discussed earlier in this chapter, the other two dimensions of social capital, the structural and relational dimension, are discussed by many researchers, and many of these discussions also provide means for linking them with shared context. Next section provides a further examination of these links.

4.3 Social capital, knowledge creation and shared context

Nahapiet and Ghoshal (1998, 244) describe the cognitive dimension to include "resources to provide shared representations, interpretations and systems of meaning among parties". Structural dimension contains all the network ties, their configurations, and the organizations they form, whereas relational dimension facilitates the interaction within these ties. All these three dimensions of social capital also have an impact on each other. (Nahapiet & Ghoshal 1998, Adler & Kwon 2000).

As discussed in Chapter 2, Blackler (1995) introduces aspects of shared context as part of the encultured knowledge, referring to the social transformation of knowledge that leads to shared, collective understandings. Nonaka (1994, Nonaka et al. 2000)

establish their process of organizational knowledge creation on an assumption that knowledge develops through socialization and combination that require a shared context, and that this shared context is also one of the outcomes of knowledge conversion. This indicates that shared context is also connected to all the four conditions of knowledge exchange and combination: access to knowledge, anticipation of value, and motivation all need to exist simultaneously in the parties involved, and combination capability itself can be seen as a manifestation of shared context. Whereas shared context is linked to knowledge creation and its conditions, it is also linked to social capital. Next sections will discuss three representations of shared context in the light of the three dimensions of social capital: knowledge overlap (redundancy), knowledge assets, and “ba” (Nonaka 1994; Blackler 1995; Grant 1996; Cook & Brown 1999; Nonaka et al. 2000)

4.3.1 Shared context and knowledge overlap

Shared context is often described as collective or common knowledge. Nonaka et al. see that knowledge and knowledge creation as such are part of a dynamic process that on its behalf transcends the existing boundaries of individuals and organizations as it based on the interaction between individual and collective knowledge. They propose that organizations have an underlying collective identity, and individuals also interact with this identity. (Nonaka et al. 2000, 14-15). Also Grant (1996) puts strong emphasis on the significance of overlapping/common knowledge in organizations: it is needed to enable social interaction and exchange. Grant (1996, 115) describes this as “the intersection of organization members’ individual knowledge sets” whereas Nonaka et al. (2000) see this more as a collective phenomenon and use the word “redundancy”.

Both Nonaka et al. (2000) and Grant (1996) see that this overlap can be a conscious choice and that it could be promoted through organizational structures. Knowledge overlap and common cognitive ground are an essential prerequisite of knowledge exchange and combination, as they enable the shared context and help the parties involved in the exchange and combination by improving the ability to understand each other’s perspectives and creating mutual trust and respect (Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003). Managers have an important role in structuring and balancing the content of organizational knowledge

(the balance between tacit and explicit) but also in ensuring the capabilities exist to leverage knowledge (Gold et al. 188-189).

Knowledge overlap can also be considered as an example of how all the three dimensions of social capital impact each other. Overlapping knowledge facilitates knowledge combination and exchange, and it is manifested through the shared resources within the cognitive dimension of social capital. It also increases shared understanding between the parties, which on its behalf increases trust – which is part of relational dimension of social capital. Knowledge overlap can be proactively developed and balanced through structural dimension of social capital. (Nahapiet & Ghoshal 1998, 243-245; Nonaka et al. 2000; Fong 2003)

4.3.2 Shared context and knowledge assets

Shared language, codes, and narratives, which can be seen as manifestations of shared context, are needed to enable combination capability. Besides these, structural and relational capital are essential in ensuring access to knowledge, forming the anticipation of value created in exchange and combination, and to motivate parties to get engaged. (Nahapiet & Ghoshal 1998).

Nonaka et al. see that such a shared context can be promoted intentionally, and their three elements of knowledge creation (introduced as part of the section 3.2.3) are describing this idea. In this approach, they consider SECI model to describe the actual knowledge creation, knowledge assets to act as inputs, moderators, and outputs of knowledge creation, and “ba”, indicating a “shared context in motion”. (Nonaka et al. 2000)

Shared context is created with the help of knowledge assets, and knowledge assets on their behalf form the organizations body of knowledge discussed in Chapter 2 (Cook & Brown 1999). Nonaka et al. identify four types of knowledge assets: 1) Experiential (tacit) knowledge (individual skills and know-how, love, trust, security, and care, as well as energy, passion and tension); 2) Routine (tacit) knowledge assets (know-how in daily operations, organizational routines, and organizational culture); 3) Conceptual (explicit) knowledge assets (product concepts, design, and brand equity; and 4) Systemic (explicit) knowledge assets (documents,

specifications, manuals, databases, patents, and licences). (Nonaka et al. 2000, 20).

Knowledge assets based on tacit knowledge, such as trust, organizational routines and organizational culture remind the elements included in the relational dimension of social capital, whereas conceptual knowledge assets and systemic knowledge assets are materializations of cognitive dimension of social capital (Nahapiet & Ghoshal 1998; Nonaka et al. 2000). Fong (2003) introduces a practical use of conceptual knowledge assets, describing the supporting role of boundary objects in project-related knowledge creation.

4.3.3 Shared context and “ba”

Chapter 2 concludes that knowledge is constantly evolving, as it constructed and formed through social interaction, relating to time, place, and wider context, and always subject to individual interpretations. Whereas the body of knowledge and knowledge assets are a manifestation of organization’s knowledge, the context of specific knowledge is also related to the time, space, and the wider context (for example the prevailing circumstances). (Nonaka 1994; Blackler 1995; Spender 1996; Cook & Brown 1999; Nonaka et al. 2000). As an enabler of access to knowledge between individuals, and to create a momentum for mutual exchange and combination within a certain context, Nonaka et al. introduce a time and space bound shared context that they call “ba”. (Nonaka et al. 2000, 25-29).

Unlike the longer term, established common ground required for continuous knowledge creation, “ba” is rather described as a temporary collection of ongoing activities and pre-set conditions. The parties involved in knowledge creation bring their own individual contexts into this shared context of “ba”, the conditions of which then help pursue knowledge creation through SECI process. (Nonaka et al. 2000, 25-29). The role of “ba” as a shared context is to act as a platform for knowledge conversion; it acts as a space where an individual contexts can be brought together, and the boundaries between those contexts can be transcended to enable knowledge creation (Nonaka et al. 2000, 25-29).

The role of “ba” itself cannot be clearly described with the help of Nahapiet & Ghoshal’s (1998) three dimensions of social capital. However, as it provides a

shared context, it can be linked with the cognitive dimension. On the other hand, it also connects the individuals, and is thereby also connected to the structural and relational dimensions. “Ba” is also plural in a sense that many “bas” can exist at the same time, and on different levels of organization, and they can be connected to each other or even overlap, in a similar way as Nahapiet & Ghoshal describe the network ties and the related network configuration. An individual “ba” thereby creates access to certain knowledge at certain time by forming a temporary network between individual contexts. As it is established for certain purpose, it includes a shared norm of functioning according to its purpose. (Nahapiet & Ghoshal 1998, Nonaka et al. 2000).

What makes ba particularly interesting is how Nonaka et al. (2000) see it should be “energized”, and they present five conditions that “ba” needs for serving its purpose: 1) autonomy; 2) creative chaos; 3) requisite variety; 4) love, care, trust and commitment; and 5) redundancy. Autonomy is defined as a possibility to self-organize, whereas creative chaos is explained as stimulation of interaction between the organization and external environment. Among these conditions, autonomy is offered to generate individual motivation for knowledge exchange and combination, whereas creative chaos means intentional triggering for creating the need for exchange and combination (Nonaka et al. 2000). Autonomy can be considered as a source of motivation, whereas creative chaos is created to both generate the anticipation of value and motivation (Nahapiet & Ghoshal 1998; Nonaka et al. 2000).

Requisite variety means balancing the organization’s internal diversity with the complex and multifaceted external environment, and thereby maintain proactive and flexible approach in knowledge creation. Nahapiet & Ghoshal mention diversity as a prerequisite for innovations but they also see that common cognitive ground is needed to overcome potential barriers arising from this diversity. (Nahapiet & Ghoshal 1998; Nonaka et al. 2000, 25-27).

The two remaining conditions can also be identified in Nahapiet & Ghoshal’s three dimensions of social capital. Love, care, trust and commitment on their behalf are part of Nahapiet & Ghoshal’s relational dimension of social capital. Finally, redundancy refers to intentional overlapping of information that helps create the

shared context mentioned also in Nahapiet & Ghoshal's work. (Nahapiet & Ghoshal 1998; Nonaka et al. 2000, 25-27).

Based on this the three dimensions of social capital can be recognized within "ba": 1) the "ba" itself is an organization or a network of individual contexts (structural dimension); 2) "ba" is functioning through commitment, trust, love and care as well as a shared purpose which acts as its norm (relational dimension); and 3) "ba" transcends boundaries between individual contexts by acting as a shared context and purpose (cognitive dimension). (Nahapiet & Ghoshal 1998; Nonaka et al. 2000).

4.4 Summary of social capital and knowledge creation

As discussed in this chapter, knowledge creation requires that four conditions exist before it can take place. Three of these conditions, access to knowledge, anticipation of value and motivation, act together to bring together the different parties, whereas the fourth condition, combination capability needs to be in place in order for the exchange and combination to succeed. (Nahapiet & Ghoshal 1998).

The four conditions are impacted by the three dimensions of social capital. Structural dimension contains the network ties, network configurations and the various forms of organizing, in which the knowledge content is created, and which establish the access to knowledge but also impact the anticipation of value as well as motivation. Relational dimension, including trust, norms, obligations, and identification, has an impact on how the individuals behave as part of their social network, and is thereby linked to both anticipation of value and motivation, but can also promote or hinder the access to knowledge. Cognitive dimension, comprising of mainly everything that is used for creating shared representations and meaning between the different parties, is the lifeblood of combination capability, as combination cannot happen in the absence of a shared context. (Nahapiet & Ghoshal 1998; Adler & Kwon 2000).

Nahapiet & Ghoshal also state that all the three dimensions impact each other in both positive and negative ways (Nahapiet & Ghoshal 1998, 243-245). Building on this thought and reviewing other literature it seems that the shared context included in the cognitive dimension and required for combination capability is also affected by the other two dimensions of social capital. These links can be identified when examining some of the concepts introduced in knowledge management literature as

enablers or elements of knowledge creation; as explained in section 4.4.3, knowledge overlap, knowledge assets, and “ba” are all promoting the formation of shared context (Nonaka 1994; Grant 1996; Nonaka et al. 2000). Nahapiet & Ghoshal consider social capital mainly as a by-product of many activities and mention that it is bound to its context (Nahapiet & Ghoshal 1998, 261), and based on the further analysis of knowledge creation related literature, the shared context built through these activities can also be considered an outcome of organization’s social capital. As knowledge is dynamic and evolves continuously (for example as described in SECI model discussed in Chapters 2 and 3), also the shared context and social capital can be considered dynamic and continuously evolving (Grant 1996; Nahapiet & Ghoshal 1998; Bhatt 2000; Nonaka et al. 2000; Gold et al. 2001; Gupta & Govindarajan 2001; Fong 2003).

5 Research context, approach, and methodology

The main objective of this study is to understand knowledge creation in cybersecurity threat modeling workshops, and how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context. From theoretical viewpoint, previous research was examined through three research sub-questions, forming the basis for Chapters 2, 3 and 4 (see Figure 10).

Chapter 2 of this study describes the nature of knowledge, especially its many characteristics and its dynamic and context-specific nature. As a result of its dynamic nature, new knowledge is continuously being created through knowledge conversion, and it is created even without intentional supporting or facilitation activities. (Nonaka 1994; Blackler 1995; Spender 1996; Cook & Brown 1999; Nonaka et al. 2000). Review of selected literature in Chapter 3 discusses different approaches to knowledge creation, identifying SECI model and its similar variants (such as “knowledge exchange and combination”) to be commonly used for describing knowledge creation as a continuous phenomenon. (Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Alavi & Leidner 2001; Fong 2003, Pinho et al. 2012).

Literature review in Chapter 3 also shows that social system/social capital related enablers and prerequisites are more important enablers and prerequisites of knowledge creation than technological enablers. (Grant 1996; Nahapiet & Ghoshal

1998; Nonaka et al. 2000; Bhatt 2000; Gold et al. 2001; Gupta & Govindarajan 2001; Fong 2003). The role of social capital as an enabler of knowledge creation is further discussed in Chapter 4, where the connections between the three dimensions of social capital, the four conditions of knowledge creation, and the shared context are also explained (Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Adler & Kwon 2000).

Theoretical research: Literature review (Chapters 2, 3 and 4)

C. How do the different characteristics of knowledge impact knowledge creation?		B. What is knowledge creation and how does it take place?		D. How do the different aspects of social capital impact knowledge creation?	
Key theories	**Concepts**	**Key theories**	**Concepts**	**Key theories**	**Concepts**
Nature of knowledge	Main dimensions of knowledge Different types of knowledge Dynamic nature of knowledge	Knowledge creation Social capital	Elements of knowledge creation Shared context Conditions for exchange and combination	Social capital	Structural, relational and cognitive dimensions of social capital

Empirical research: Qualitative case study (Chapters 5 and 6)

E. Which elements of knowledge creation can be identified in threat modeling workshops?

Results, discussion & conclusions (Chapters 6 and 7)

A. What enables knowledge creation in threat modeling workshops?

Figure 10. Structure and approach for this study, including related theories and concepts.

This chapter describes the empirical research context and approach that was used to examine the elements discussed in Chapters 2, 3 and 4 through three case studies.

First section 5.1 briefly explains the concept of cybersecurity threat modeling. The next four sections (5.2-5.5) describe the empirical research: what kind of approach and methodologies were utilized, what kind of methods were used for data gathering and data analysis, and what kind of limitations the approach might have contained. Finally, section 5.6 describes the three threat modeling cases that were analyzed

for this research by first offering a summarized view, and then describing the specific characteristics of each case.

5.1 Research context

While the digital operations have both replaced many analogic processes and practices, an brought along new innovative approaches, also the significance of understanding and mitigating new kinds of risks, threats and vulnerabilities within the digital world has increased. The field of cybersecurity looks at digital operations from this specific angle, consisting of many types of activities that can be taken for example to prevent the cybersecurity incidents from happening or to minimize the damage caused by them. This study focuses on cybersecurity activities that aim at identifying potential threats that the systems could be exposed to, and that could eventually lead to cybersecurity incidents.

Frameworks categorizing various cybersecurity activities provide an opportunity to show where the context is situated within these activities. End-to-end cybersecurity management approach is often considered to consist of four different categories of activities (see Figure 11): 1) identify/predict the risks/threats, 2) prevent them from happening by improving cybersecurity levels (defense), 3) detect possible threats/attacks/breaches, and 4) respond with fixes and further improvements. (Gartner 2017, National Institute of Standards and Technology (NIST), 2018).

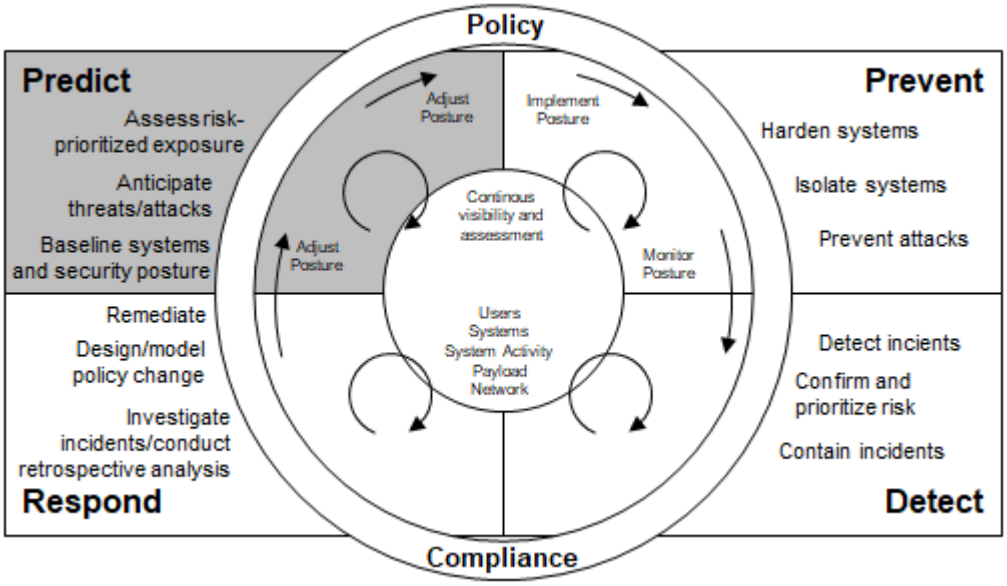


Figure 11. Cybersecurity activities and the focus of this study. (Gartner 2017).

Threat modeling is part of predictive cybersecurity activities (highlighted in Figure 11). Cybersecurity risk management approaches, methodologies and frameworks provide a feasible opportunity for organizations to understand, analyze and prioritize the risks attached to their digital structures and support them in creating mitigation plans. Threat modeling, on its behalf, helps the organization to gain more exact information on what could go wrong considering how a particular system or its function/component has been built and how it interacts with different elements (including the user). As described in Figure 11, threat modeling and other predictive activities often lead to preventive activities. (Shostack 2014; Schoenfield 2015)

Threat modeling is done with the help of two models: 1) A model of what you are building, deploying or changing, and 2) A model (or an addition to the first model) of what can go wrong. Shostack (2014) describes threat modeling as an everyday activity: whenever you are planning something, you also need to consider what can go wrong, decide whether you prepare for that or not, and if so, how. Threat modeling stages would thereby include:

1) Model the system – what are you building?
2) Find threats using the model – what can go wrong?
3) Address threats – what should you do?
4) Validate – did you do a decent job? (Shostack 2014, xxii)

There are several ways of doing threat modeling: organizations can decide on how often they threat model, what tools and techniques they use, whether they have staff dedicated to this or not, and how they manage the related work. (Shostack 2014). The high-level approach used by the facilitators involved in the workshops analyzed in this study, as well as the workshop context and flows for each of the three cases is described in Section 5.6 Case descriptions.

Organizations are usually not eager to openly share the cybersecurity activities they are applying, as this might reveal knowledge that could increase their risk exposure. Especially the content of threat modeling activities can be considered confidential information. Confidentiality requirements were maintained throughout the study, and they were supported by three decisions. First, the research focus was set on “the how” rather than “the what”, and with this decision, it was possible to leave out the

content used and created during threat modeling. Second, most of the approaches used in the case workshops are widely available for everyone (see for example ENISA, 2019 for risk assessment methodologies listed and evaluated by European Union Agency for Cybersecurity), and therefore describing them as part of this work on a high level was possible without sharing any confidential information. Finally, the confidentiality of the research context had an impact on how research material was handled and analyzed: all technical details as well as potential individual or organizational identifiers were removed when research material was processed.

5.2 Research approach and methodology

This study was conducted as a qualitative case study, and research logic was based on abductive reasoning. Empirical research material included three threat modeling workshops, each of which involved a unique scope and group of participants. This section describes the selected approach and methodology and discusses some underlying reasons behind the selections.

5.2.1 Research questions

The research objective was used as a basis for the main research question:

A. **What enables knowledge creation in cybersecurity threat modeling workshops?**

Additionally, the research motivation itself was based on an assumption that the fast pace of digital development in organizations as well as the dynamic and context-driven nature of knowledge create a need for organizations to intentionally facilitate their knowledge creation in order to be able to plan and manage their cybersecurity-related activities.

The main research question was addressed with the support of four sub-questions (Figure 12):

Addressing this question requires answering to the following sub-questions:

B. What is knowledge creation and how does it take place?
C. How do the different characteristics of knowledge impact knowledge creation?
D. How do the different aspects of social capital impact knowledge creation?

E. Which elements of knowledge creation can be identified in cybersecurity threat modeling workshops?

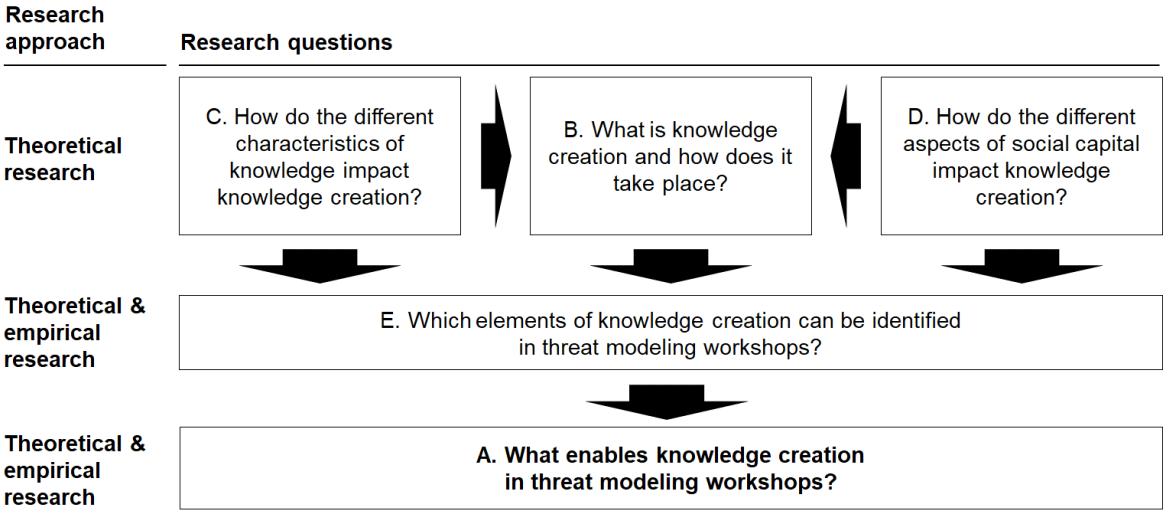


Figure 12. Research question, sub-questions and related research approach.

5.2.2 Research methodology

In this section, research methodology and approach consist of "putting together a complete and integrated research design", whereas the methods discussed in the next two sections describe "the concrete elements of steps associated with the research project". (Staller 2012, 403-405). The order in which the methodological selections are introduced follows the chronological order of the choices made when designing this research.

Case study

Case study was selected as the research methodology, as it provided an opportunity to gather data over time and with a help of more than one method. Using threat modeling workshops as a research context meant that the workshop was in the core of data gathering, and – as stated in the research objectives – the focus was more in the process (how does knowledge creation take place) than in the outcome (what knowledge is created), which indicated that an in-depth view on the researched phenomenon was needed. Case study was a suitable method for such a research setting. (Dubois & Gadde 2002; Yin 2017).

As the duration of a single threat modeling workshop was already known to be maximum half a day, utilizing several methods and extending the data gathering to take place also before and after the workshop enabled forming a deeper understanding what happened during the workshop and why. Despite the short duration of data gathering period per each case, the case study approach and the use of the additional data points besides workshops provided an opportunity to gather more in-depth information than what for example a survey or an interview research would have enabled. (Dubois & Gadde 2002; Blatter 2012; Yin 2017).

This research was approached as a multiple case study (Yin, 2017): even though all the cases were representing “a case” of threat modeling workshops, their setup differed from each other in terms of scope, participants and facilitators, and the analysis focus was within each of the workshops as a separate series of events rather than an overall case of threat modeling workshops in general, mainly to leave room to investigate the potential impact of the differences between the contexts of each case but also to enable finding similarities between the cases.

Qualitative research methods

Another choice related to the research approach was whether to use qualitative or quantitative methods for data gathering, or whether to use both. A qualitative research approach was considered more suitable for a this study, as it suits better for studying phenomena that take place through social interaction and over time – in this situation, the knowledge creation taking place between individuals within the time window of three threat modeling workshops. (Padgett 2017; Yin 2017).

Additionally, the objective of the research was more to increase the understanding on how knowledge creation takes place in a limited case-based setup (three threat modeling workshops) rather than to make any generalizable conclusions by collecting large volumes of data. This objective also affected on selecting a qualitative approach; answering the question “how” required a deeper dive into the research scope than what a quantitative approach could have enabled. Case studies typically rely strongly on qualitative research methods. (Dubois & Gadde 2002; Padgett 2017; Yin 2017).

Abductive reasoning logic

Abductive reasoning logic differs from the more traditional deductive logic (aiming at demonstrating the validity of theory through empirical evidence) and inductive logic (making theoretical conclusions based on empirical research) as it enables a continuous discussion between various theories and the empirical material to find a suitable explanations that connect some of the theories to the observations (Mantere & Ketokivi 2013; Bamberger 2018).

The decision to use abductive reasoning was rather natural considering the researcher's own background with cybersecurity industry and the lack of earlier knowledge management research done in the field of cybersecurity. As the theoretical approach started to form, using researcher's earlier observations as a sounding board supported finding a feasible set of theories to start planning the data gathering.

The decision to focus on three threat modeling workshops as individual cases required identifying various explanations between the theory and the observations. Abductive approach supported this decision, as it enabled sensitizing with multiple theories and concepts without the risk of ending up forcing all cases to same conclusions without reasonable evidence. (Dubois & Gadde 2002; Timmermans & Tavory 2012).

Case studies proved to be suitable for maintaining the abductive approach throughout the empirical research. As the data gathering proceeded, logical connections within the data gathered from the perspective of each of the cases as well as between the cases started to form, and these results were then reviewed in the context of the concepts and theories evaluated already earlier for this study. Finally, the findings were used for enriching the original set of theories and concepts. In this sense, the abductive approach provided flexibility to also report such findings that were not fully aligned with the original theories, and then to see whether these findings would have any theoretical base. (Dubois & Gadde 2002; Tuomi & Sarajärvi 2009, 96-97; Timmermans & Tavory 2012).

5.2.3 Research approach

At the beginning of the research, a literature review was conducted identify initial answers to three of the sub-questions and to anticipate potential structure and methods for empirical data gathering. For this purpose, mainly the theories of knowledge creation, nature of knowledge and social capital were examined (see Figure 13). Initial findings from the literature review were then used for creating an initial theoretical framework, describing the potential elements of knowledge creation, and to form an understanding of the three research questions:

C. How do the different characteristics of knowledge impact knowledge creation?

B. What is knowledge creation and how does it take place?

D. How do the different aspects of social capital impact knowledge creation?

Theories and concepts related to these questions were used as a basis for Chapters 2, 3 and 4 of this study.

Based on the initial theoretical framework, the structure for the empirical research approach was then designed with an initial objective of gathering data for answering the fourth sub-question:

E. Which elements of knowledge creation can be identified in cybersecurity threat modeling?

The empirical data was gathered from three cases (cybersecurity threat modeling workshops) as a qualitative inquiry. Primary research data was gathered both through workshop observations and semi-structured interviews of workshop facilitator and owner before and after each workshop. Workshop presentations and documentation were used as secondary data and to complement primary research data. Data gathering and the used methods are further described in section 5.3.

Research material was analyzed both by identifying emerging themes and reflecting the findings with the help of theories and concepts, that were also abductively enriched during the process. Chapter 6 was formed based on this analysis. Finally, the results of this reasoning were reflected to the research questions to form research conclusions discussed in Chapter 7, and to answer the main research question

A. What enables knowledge creation in threat modeling workshops?

The end-to-end research approach described above is also summarized in Figure 13, and data analysis and the used methods are further described in section 5.4.

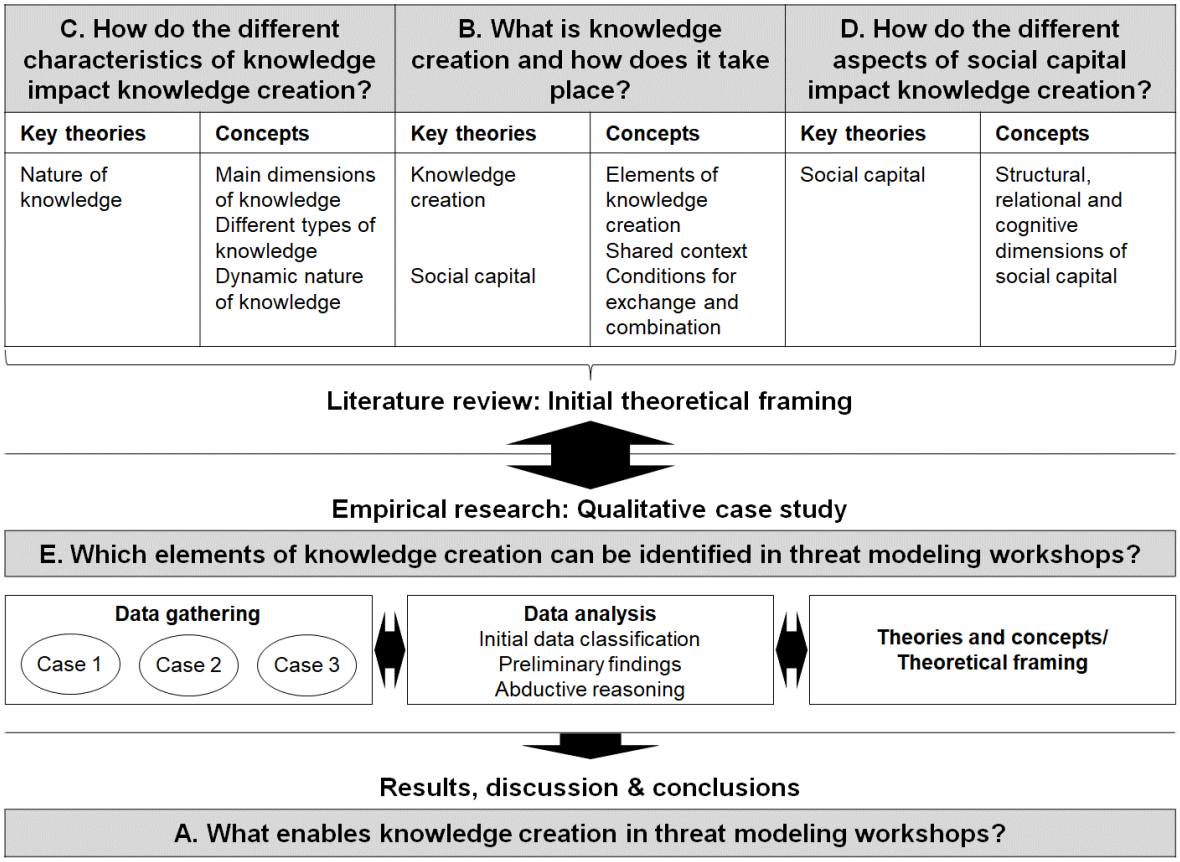


Figure 13. End-to-end research approach.

5.3 Data gathering approach and methods

The empirical research material was gathered through three separate cases, each representing one cybersecurity threat modeling workshop. Cases included in the research were decided jointly with the respective facilitators. Each case consisted of a workshop and interviews with the workshop owner and facilitator both before and after the workshop.

Primary data gathering was done in three phases (see Figure 14):

1) Semi-structured, individual focus interviews with the workshop owner and the facilitator before the workshop
2) Workshop observations during the workshop

3) Semi-structured, individual focus interviews with the workshop owner and the facilitator after the workshop

The facilitator of the respective workshop briefed the owner of the workshop about the research, and the researcher then contacted them to agree the practicalities for the interviews and workshop observations. The primary data was gathered over a period of three weeks (see Figure 14).

	April 2020													
	3		6	7	8	9		14	15	16	17		20	21	22
Case 1 Pre-session interviews Workshop Post-session interviews	O			F				(PM)					WS F		O
Case 2 Pre-session interviews Workshop Post-session interviews				F	O				WS	F,O					
Case 3 Pre-session interviews Workshop Post-session interviews						F		O	WS	O			F		

O = Owner interview; F = Facilitator interview; (PM) = Preparatory meeting including facilitator & owner; WS = Workshop.

Figure 14. Timeline of interviews and workshops used for empirical research.

Besides the workshop observations, a preparatory meeting between the facilitator and the owner for case 1 workshop was observed for research purposes. Additionally, the documentation presented and created during the workshops was used as secondary research material for each case to complement the data gathered through the interviews and workshop observations.

5.3.1 Workshop observations

Workshop observations were used as the main method for gathering data on knowledge creation during threat modeling workshops. Especially in an onsite setup, observations provide an in-depth access to both the context and the phenomenon to be researched (McKechnie 2008).

The workshops observed for this study were held online, and enabled to record the discussions. Additionally, the material shared, and the separate text-based chat discussions conducted during the discussions were also observed. Compared with traditional field observations, observing online workshops did not provide an

opportunity for observing expressions or gestures, as the participants did not use video connections.

Before the workshops, each owner briefed the participants on the planned observation approach as well as the intention to record the workshop for research purposes. The researcher was briefly introduced at the beginning of each workshop but remained otherwise as a silent observer throughout the session.

The workshops were recorded with an online meeting tool, and as the tool did not provide an opportunity to record chat discussions or – in those cases where it was used - the use of an online whiteboard tool, the researcher also took screenshots during the workshops. All three workshops were held in English and the recordings were transcribed and anonymized after the workshops. Both the planned and actual duration for Case 1 workshop was 120 minutes, whereas for Case 2 workshop it was 105 minutes and Case 3 workshop 90 minutes.

5.3.2 Semi-structured focus interviews

Besides the data gathered in the actual threat modeling workshops, workshop owner and facilitator interviews before and after the actual threat modeling workshop were used to gain deeper, more insightful data on each of the cases.

Semi-structured focus interviews were used as a method for both pre- and post-workshop interviews, as this method provided an opportunity to ask open ended questions and still to compare the input gathered both interviewees (the owner and the facilitator) in each case. Using for example interview forms instead would have likely produced too little information, as the objective was to understand causal relationships and social interaction. (Hirsjärvi et al 2007; Ayres 2008; Tuomi & Sarajärvi 2009).

Both pre-workshop and post-workshop interviews were following a pre-planned high-level structure that was also used as a support in the data analysis. Instead of a traditional, more positivist way of structuring the themes based on the theories and concepts, a chronological structure following the workshop from the preparations to the event and then to the output was chosen, as this approach was considered to better fit the abductive analysis approach assumed for this study. (Ayres 2008).

There were altogether four interviews per each case: the facilitator and the case owner were interviewed separately before and after the session. From the total of twelve interviews, ten were held in Finnish and two in English. The average duration for the interviews was 47 minutes. All the interviews were held online and recorded with an online meeting tool. In case of Finnish interviews, the recordings were first transcribed in Finnish, and then anonymized and translated into English.

In addition to the interviews, also a separate preparatory meeting of Case 1 between the facilitator and the owner was used as research material. The meeting was held in Finnish, and it was recorded, transcribed, anonymized and translated in a similar manner as the interviews.

Pre-workshop interview structure

Pre-workshop interviews started with questions regarding the background for the workshop, mainly to understand why it was held and how it had been initiated. Going forward, the discussions went through the preparations from the viewpoints of workshop timing and place, participant selection and the related reasoning, as well as planning the actual workshop. Finally, the expected deliverables and outcomes were discussed.

Pre-workshop interview structure, including the research questions and underlying theories and concepts can be found in Appendix 1.

Post-workshop interview structure

Post-workshop interview structure consisted of similar elements as the pre-workshop interview. The main focus was on how the workshop was conducted, what kind of contribution the interviewee brought up, how their expectations were met, and what would happen after the workshop. Positive aspects and benefits, feedback and development ideas regarding the workshop were also discussed.

Post-workshop interview structure, including the research questions and the underlying theories and concepts can be found in Appendix 2.

5.4 Data analysis and methods

Data analysis started already in the data gathering phase by sensitizing the theories examined for literature review based on the observations done during the

workshops and interviews, and it also continued during data transcription. The research logic followed abductive reasoning, and this materialized in the continuous interaction between theory and the empirical research material throughout the analysis. (Dubois & Gadde 2002; Padgett 2017).

The actual data analysis started with the identification of potential classification themes emerging from the research material. Besides reading through the material for this purpose, also the themes and theories included in the research questions were utilized for this purpose. Altogether four main themes emerged, and the research material was then classified under these themes with the help of color coding. As part of this work, theoretical analysis was completed with additional aspects. The outcome of the coding phase is summarized in section 1 of Chapter 6.

After the initial findings were categorized in themes, they were then sensitized with the theories and concepts discussed in Chapters 2, 3 and 4 (also listed in Figure 13). As part of this analysis, the set of theories and concepts was further clarified. The initial observations from the empirical research were then reflected with the set of theories and concepts resulting from these iterations to identify mutual connections. These connections are explained in Chapter 6. Finally, the findings emerging from the data as well as the experiences from the analysis process were used as a basis for the research discussion and conclusions in Chapter 7. To provide a deeper insight on the research material, separate case walkthroughs were created and added into section 5.6.

Before finalizing the research report, the case walkthroughs, results, and key findings were shared with the facilitators interviewed for this study. This was done mainly to ensure no confidential data would be used within the research report, but it also provided an opportunity for the facilitators to suggest amendments in case of any misunderstandings had been made by the researcher. This review resulted in two small amendments which did not have any impact on the findings or conclusions of this study.

5.5 Research reliability and validity

The research approach selected for this study included several risks and reservations that may have impacted the quality of this research. As a contrast to

quantitative research having somewhat clear criteria for reliability and validity, evaluating qualitative research should be based on its trustworthiness and rigor (Padgett 2017). The criteria for qualitative study evaluation often consist of transferability, credibility, dependability, and confirmability (Given & Saumure 2012). However, there are also several other criteria that can be used for evaluating qualitative research (Patton 2012).

Transferability means evaluating whether the findings would be potentially applicable in other research contexts (Given & Saumure 2012). Regarding this case study, the findings were already in advance expected to primarily apply to describe the cases included in this research.

The neutrality of the individuals involved in the research is considered as one of the underlying factors of its trustworthiness (Padgett 2017), and this can be seen as a part of what is called the research confirmability in terms of unbiased data (Given & Saumure 2012). The background of the researcher and its potential impact on the study were stated openly during the research and within the related report.

In a research where data gathering is done using interviews, the selected data gathering may also impact the research objectivity and confirmability. Due to the researcher having some background in the field of cybersecurity as well as them being familiar with some of the interviewees may have impacted in the research objectivity three ways: 1) interviewees may have been more open to an interviewer that was considered as a colleague rather than a researcher; 2) researcher's background may have impacted the interview situation, for example in the way of asking clarifying questions based on their own previous experience, and 3) interviewees may have expected the researcher to understand their input (and vice versa) due to the previous shared experiences, and thereby may have left out additional information that would have clarified their input (Berger 2013).

Using several data gathering methods and studying three separate cases created a situation where the analysis and data gathering partly overlapped – for example the data gathered during a pre-workshop interview likely had an unconscious impact on what was observed during the workshop, and transcribing the interviews while the data gathering was still ongoing unavoidably also led to at least initial processing of

that data also from an analysis point of view. This is typical for case studies but should be considered when evaluating the neutrality of the analysis. (Dubois & Gadde 2002; Blatter 2012; Yin 2017).

Another form of evaluating research confirmability is to look at how the interpretations and findings done in the research match the observations (Given & Saumure 2012). Both the beauty and the unpleasantness of using abductive analysis approach are linked to its flexibility and permissiveness (Bamberger 2018): while the phenomenon studied in this research itself was rather ambiguous (at least based on the previous literature) and the selected abductive approach also enabled continuous interpretations and alterations to be made throughout the research, it may be questioned whether the research setting itself had even allowed evaluating whether the outcomes are confirmable or non-confirmable. Hence, in the context of abductive reasoning, the research was considered confirmable.

Besides its potential implications on the reliability of this study, the abductive reasoning logic may have also had an impact on the credibility of the results when combined with the selected data gathering approach. As the research context contained three cases, each representing a slightly different context of threat modeling but also including similarities, it can be argued whether the data gathered through these cases formed a representative set of observations. As the cases were based on workshops that only lasted for maximum two hours, and also the interviews were done within a relatively short timeframe (see Figure 14), also the time available for abduction during the data gathering period was relatively short. Additionally, the applied approach did not include an opportunity to revisit the research context to further validate the theories and concepts emerging from the data analysis. A longer research timeframe and a longitudinal case study would have probably provided better opportunities for abductive reasoning and may have resulted in additional findings and further theoretical explanations for the observations. (Visconti 2007). However, as the research objective was to understand knowledge creation in the context of threat modeling workshops by using these three cases as a research material, it provided credible findings within this research context.

Finally, research dependability should be evaluated in terms of whether the research design allows repeating a similar research within similar conditions (Given & Saumure 2012). As the research design was strongly based on the abductive reasoning logic, the research as such was not intended to be repeatable.

5.6 Case descriptions

The empirical research material was based on three separate threat modeling workshops, each of which is approached as its own case in the analysis. On high level, all three threat modeling workshops followed the same four-phase approach. As the need for threat modeling had been identified, it was recorded into the work management system (1). Then the workshop was prepared (2) and conducted (3) and finally, the actions were recorded into the work management system (4). The high-level approach is described in Figure 15.

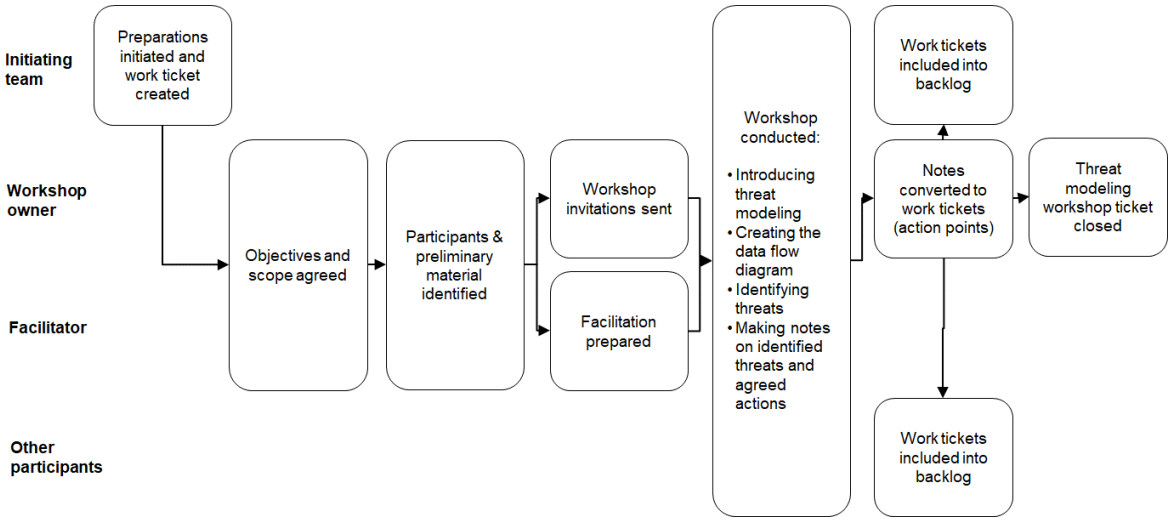


Figure 15. High-level approach for planning and conducting a threat modeling workshop.

When the threat modeling need was first identified by an individual or a team, they recorded this need as a work ticket into their work management system. At this stage, the ticket included a short description of the initial scope for threat modeling as well as the owner for the initiative. As part of this, they had also decided they would benefit from using an external facilitator to support them with the workshop, and they had contacted the facilitator. Another option for the team or the individual would have been to do the threat modeling on their own.

This was followed by a discussion between the facilitator and the owner on the objectives and scope for threat modeling. When they found the objectives and scope to be clear enough, they also identified who they would need to involve to reach the objectives regarding the set scope. They also preliminarily agreed on who of the participants would be modeling the scope (the “drafter”) and who would be taking the notes during the workshop (the note taker). Based on the discussions, facilitators also planned the preliminary approach in terms of which facilitation tools and methods they would use during the workshop. They needed to think about what kind of model (data flow diagram, message sequence chart, or some other model describing the system in scope) would suit for the purpose, as well as what kind of a approach/guideline they would use to facilitate the discussion and to ensure the majority of relevant types of threats would be covered.

After the initiation and preparation phases, the actual threat modeling workshop took place. On a generic level, all the three workshops had a similar structure consisting of four steps: introduction (including the objectives, scope, threat modeling approach and workshop roles), drawing a model of the scope, identifying threats related to the scope, and agreeing upon next steps.

In all three cases, the scope was modelled with the help of data flow diagrams that described the flow between the different elements within the scope. In all three workshops, also several other aspects such as data types, storages, formats, process steps, interfaces and boundaries, as well as their characteristics such as level of automation were documented into the diagrams. Appendix 3 includes a generic description of a data flow diagram and what it can contain.

Facilitators also used the same approach, a model called STRIDE to support in threat identification in all three cases. STRIDE is an abbreviation of six different threat categories: spoofing, tampering, (non-) repudiation, information disclosure, denial of service, and elevation of privilege, and it was described to act as a reminder for the facilitators, even though they would not follow through it in a structured manner during the workshops. Appendix 4 includes a more thorough description on each of the STRIDE model elements.

For all workshops, the owner ended up taking the notes during the discussion. Potential threats as well as the actions identified during the workshop were recorded in the notes. The facilitators explicitly stressed during the workshops that the objective was to identify threats and issues and that the solutions should have been created only during the next steps after the workshop.

The fourth and the final phase that still could be considered as part of the threat modeling workshop was to ensure the progress. The threat modeling workshops and the related work recorded in the work ticket was considered done based on two conditions: 1) the workshop documentation was included in the work ticket created for the workshop, and 2) the identified threats/issues and actions were visible in the backlogs of the related teams, and linked to the original workshop ticket. Appendix 5 includes a summary of the documentation related to threat modeling workshops.

Table 4 summarizes the three cases in terms of their high-level scopes and objectives, participants, and deliverables. Next, each of the cases will be described in more detail.

Table 4. Summary of the cases.

Case	Scope and objectives	Initiated by	Workshop owner	Workshop participants (#)*	Cross-team workshop?	Deliverables
1	Identifying threats for third-party SaaS solution used for business operations, introducing threat modeling approach to the team	Solution team lead	Solution team lead	Solution team, excluding developers (Total 5)	No	Data flow diagram (drawn on digital whiteboard) Notes (digital format)
2	Identifying threats for building a direct interface between two third-party SaaS solutions	R&D team member using both solutions and having a need for the new interface	R&D team lead	Initiating R&D team, selected stakeholders from both third-party solution teams and additional participants from various teams (Total 20)	Yes	Data flow diagram (drawn on digital whiteboard) Notes (digital format)
3	Identifying threats regarding a new functionality of a SaaS product developed by the company	Product team together with the Quality lead for the business unit	Quality lead for the business unit	Selected product team members and developers, portfolio project manager, quality lead and quality engineer (Total 9)	No	Data flow diagram (drawn on analogical whiteboard, shared as a photo) Notes (digital format)

* Facilitator excluded.

5.6.1 Case 1 description

Case 1 threat modeling workshop was conducted with a team that was responsible for running and developing an important business operations related system. The organization in question had been working with the solution for a couple of years already, developing it both in co-operation with the solution provider (third-party vendor) as well as internally based on the business requirements. Some interfaces to this system from some other systems had been threat modeled previously but this threat modeling was supposed to be the first one to be focusing on the solution itself and the potential threats embedded into its functional scope and interfaces.

Solution owner was acting as the initiator and the owner for threat modeling. They were leading a solution team which had been organized so that each of the three sub-elements of the solution, A, B and C, had dedicated sub-owners. The sub-owner of element C was planning to move to another position outside the team, and the team had already identified that the current business analyst, D would assume sub-owner C's responsibilities when this would happen. The solution owner themselves had the overall responsibility of the solution.

The solution had been first taken into use several years before, and its elements had been developed somewhat separately. The overall solution owner had just recently combined all the development responsibility of all the three elements into one team. Since then, the solution team had been improving security based on their own activities as part of their daily work, and some of them had participated in cross-functional threat modeling workshops. Also, the solution provider had arranged trainings and shared guidelines and documents related on how to build an improve security for the solution elements.

The solution was considered such a large entity that several threat modeling workshops would be needed. The plan was that if and when the most critical interfaces of the solution to other systems and solutions would have been identified during the first workshop, it would be likely that stakeholders from other teams would be involved in the next workshops, or at least be contacted, in case the team would identify any potential threats lying in these interfaces.

Case 1 pre-workshop activities

At the earlier preparations it had been agreed that the objective for the first threat modeling workshop would be to describe and understand the overall picture of the solution and to decide, where to focus then with the next threat modeling sessions. As another, longer term objective they mentioned that their team had been identifying potential threats as part of their daily work and that they would like to start doing this in a more structured manner; they mentioned that the session would act as a starting point for this, as it would introduce some new approaches for threat identification. The team had also been familiarizing themselves with the security aspects of the third-party solution in question as part of the trainings and guidelines provided by the solution provider.

The workshop had been postponed several times due to scheduling difficulties, and the facilitator and the owner agreed on an additional pre-workshop meeting to ensure they still had a mutual understanding of the scope, the agenda and the expected outcomes of the first session as well as all the preparations in place for the session. This meeting, that was also monitored for the research purposes, concluded that the session should focus on three agenda elements: 1) introducing threat modeling as an approach for the team, 2) drawing a data flow diagram describing the interfaces and main business processes of each of the three main solution elements, and 3) focusing on threat modeling on element C, as the current owner of this element was moving to another role, and the workshop was also considered as a possibility for knowledge transfer regarding element C.

Regarding other preparations, the owner planned to ask the participants to prepare to the session by listing the relevant items from their responsibility areas' perspective. The facilitator ensured a setup for an online workshop and shared information about the related tools with the team. The owner shared existing solution documentation with the facilitator.

Case 1 threat modeling workshop

In addition to the solution owner, workshop participants included the three sub-owners for each solution element (A, B and C), as well as the business analyst D

who was planned to take over the responsibility of sub-element C in a few months. Workshop duration was planned to be two hours (120 minutes).

The workshop started with introductions and allocating the roles of a drafter (person to have main responsibility for drawing the data flow diagram), into which D volunteered, and a note taker, which was agreed to be done by the owner. After the introductions, the facilitator introduced threat modeling approach, including why it is done, how it is usually done (including an introduction to various tools and methods, including a data flow diagram and STRIDE model), and what is expected from a team during and after a threat modeling session. They also reminded participants to keep an open mind and trying to avoid potential thinking bias (by giving an example of these). Finally, they explained their own role in the workshop, they also suggested to the team that in addition to bigger workshops and sessions, “light-weight threat modeling” should always be done as part of daily work whenever there are even small changes proposed

The workshop continued with a discussion on the scope. During the discussion, it was agreed that instead of creating first a high-level description of the whole solution including all the elements, the workshop should focus on sub-element C instead. Participant C, who was the owner of sub-element C at the time of the workshop, went through what should be included. The team then proceeded by defining use cases for sub-element C.

After some challenges with the online tool, the drawing started. Participant D started to draw the data flow diagram describing element C, and participant C was explaining to participant D how the process works. The drawing was also supported with questions and comments by the other participants, the owner, and the facilitator. As the online tool enabled two people to draw simultaneously, facilitator also added the comments to the diagram while C continued drawing. Regarding those questions that could not be answered, facilitator suggested the question would be put into notes and clarified with those stakeholders that would know about the topic. When the diagram started to appear to be ready, facilitator asked for final comments from the participants before moving into threat modeling phase.

Threat modeling started with a discussion of use cases, and the participants explained the differences between different use cases to the facilitator. Based on this discussion, facilitator suggested drawing some additional system boundaries to the data flow diagram to better understand which parts of the system entity were on the responsibility area of the team in question. The team selected the first use case to be used in threat modeling.

Facilitator then continued by explaining the first element of STRIDE model, spoofing, and the discussions started. The workshop progressed mostly according to the STRIDE model structure, and the facilitator explained and gave examples on different types of threats to the participants during the modeling. Whenever there was something outside the team's own responsibility area, this was noted separately. All the issues that were identified during the discussion were recorded in the notes. Facilitator supported the discussion by asking a lot of open questions addressed to everyone and encouraged participants A and B to bring in their insight even though the sub-element was not on their responsibility. Whenever the team started to discuss a potential solution for an identified threat, facilitator steered the discussion back to threats. The owner also contributed into the discussion, and besides commenting on the threats, they also clarified whenever the identified threats were linked to already existing tickets and made notes to add the input into those. For those threats that were outside the team's scope, notes were taken so that tickets could be created to ensure validation and further discussions. The owner also checked regularly whether they had managed to capture all the relevant notes.

When the team finally agreed that the analysis was more or less done, they agreed on saving and sharing the meeting notes. They also commented that the workshop had focused on practicing threat modeling, and that the more the team would do this the better they would become in drawing the diagrams and discussing the threats. The facilitator ensured the owner will convert the notes into actions and work tasks. Some additional notes were still taken as part of the closing discussions, mainly related to preparing for the next workshop. The owner and the facilitator agreed that the facilitator would support the owner in finding a suitable way to convert the notes into actions. The workshop ended within a planned time with a feedback round and

a recap of next steps. Case 1 workshop phases and participation are described in Figure 16.

Workshop phase	Introduction	Creation of data flow diagram	Threat identification	Workshop summary and closing	Total
Duration of the phase	34’	23’	52’	12’	121’
Active participants	• Facilitator • Owner (team lead) • Sub-owners A, B & C • Business analyst D (the drawer)	• Facilitator • Sub-owner C • Business analyst D (the drawer) • Owner (team lead)	• Facilitator • Sub-owner C • Business analyst D (the drawer) • Owner (team lead) • Sub-owners A & B	• Facilitator • Owner (team lead) • Sub-owners B & C • Business analyst D (the drawer)	5 active participants (total 5 participants, excluding the facilitator)

Figure 16. Case 1 workshop phases and participant activity.

Case 1 post-workshop activities

After the session, the owner shared the notes with the rest of the participants and updated the work ticket related to the threat modeling workshop. The facilitator arranged a feedback session with the team on how the workshop went and how to plan the next one. For this purpose, the facilitator had also made some notes for themselves on how to develop the approach for the next workshop with the team in question.

The plan was that the solution team members would continue to work on the tickets they were able to take forward, whereas the owner was intending to discuss with the stakeholder teams identified during the workshop and create tickets for their backlogs regarding on those few findings that were not under the team’s own control. The owner emphasized that as the solution is used by internal users in many functions, any changes into the processes and functionality that may arise from the findings also needs to be shared and discussed with the users.

5.6.2 Case 2 description

Case 2 was based on a change requirement that one of the many R&D teams of the organization in question had identified as part of their daily work. The R&D team member who had identified this requirement was working with two different third-party solutions on a daily basis, and they had started to think that having a direct interface between these two solutions would make their work faster and reduce the probability of mistakes.

They had posted the requirement as a work ticket to the team managing one of these solutions, and – as this was considered to be a change request to the current setup – they had responded that the proposed change should be evaluated also from the security viewpoint. Based on this feedback, the R&D team lead had created a threat modeling ticket, contacted the facilitators and started the discussions about arranging a threat modeling for the proposed change.

Case 2 pre-workshop activities

The facilitator and the workshop owner, who was the lead for the R&D team initiating the threat modeling, had held some preparatory discussions to identify the scope and the objectives for the threat modeling session. The objective for the session was to identify potential threats linked with the R&D team's requirement so that the team could get some input. The intention was that after the workshop, they would further analyze the threats and their impacts, and add this information as an input to the requirement work ticket they had already made for the team that was responsible for the system; aka use the information as one of the inputs for decision-making on whether the change request/requirement could be implemented.

The workshop had already been scheduled once, but as the preparations had proceeded, it had become clear for both the owner and the facilitator, that the R&D team (the owner's team) itself would not have been able to do the threat modeling by themselves, as they were the users of the third-party solutions in question and were not having the adequate understanding on how those solutions had been built. The workshop invitation was extended to include the selected key stakeholders from the third-party solution teams, and it had taken a while to find a new timing that would suit everyone. Even though the person who would decide whether the change would be implemented would be one of the key stakeholders who had been added to the participant list for the workshop, the intention was not to make any decisions during the workshop but only to identify potential threats.

The duration of the session was planned to be one hour and 45 minutes (105 minutes). According to the facilitator, the duration was based on an assumption that the third-party solution teams would have had a similar change already implemented with some other teams, and that this particular session only required identifying the

differences (stated as “gaps”) between the already existing implementations and the one that would now be analyzed in the upcoming session. As a preliminary information for the participants, the calendar invitation for the workshop included a link to the work ticket, containing the original change request and the description of the requirement. Besides this, the facilitator informed that they had asked the R&D team member, who had been initiated the request, to prepare a draft of data flow diagram including the current setup of the R&D team work and relevant interfaces and data flows.

The owner and the facilitator had slightly differing expectations for the workshop. The owner was interested in understanding the threats linked to the proposed change, but also in the opportunity it would provide to their team in terms of widening their perspective from their own operations to the “systems that surround us, the network limits, firewalls, routing and so on”. The facilitator, on their behalf, was also looking forward to understanding whether the scope would prove to be even bigger than what had been discussed. Both third-party solutions were used widely also by other R&D teams of the organization, and according to the facilitator, the extended group of participants was also needed to ensure the findings from the workshop can be used for evaluating threats arising from building the direct connection the two third-party solutions in potential other situations.

Case 2 threat modeling workshop

The workshop was held online, with a help of a meeting tool and an online drawing tool. Workshop participants consisted of the team lead (the owner) and team members from the initiating team (R&D team), as well as the head of the teams managing both third party solutions used by the R&D team (who was also the decision-maker for implementing the request afterwards), and various members of both third party solution teams. One of the original invitees had not been able to join, and instead forwarded the invitation to their team members, many of which had joined the online workshop.

The workshop started with introductions and going through workshop roles, the facilitator, the drafter and the note taker. It had already been agreed prior to the workshop that the owner would act as the note taker and that the R&D team member

would be responsible for the data flow diagram. During the opening it was made clear that many of the participants did not have any previous experience on threat modeling. Facilitator went through an introductory presentation, explaining why threat modeling is usually done, how it can be done (presenting the tools and methods, including the data flow diagram and STRIDE in more detail), what kind of cognitive bias or attitudes can prevent identifying threats, and what would be expected from the participants during and after the workshop. They also emphasized the learning and knowledge sharing possibilities as well as the collaborative nature of the session, stating that it would be a good opportunity to validate assumptions each of the participants would have regarding each other's work. They further explained how the potential findings and remarks recorded in the notes would be converted into work tasks for the teams after the workshop.

After this, the workshop continued with the drafter explaining the initial data flow diagram they had prepared for the workshop. This was followed by clarifying discussions of the diagram, its different elements and the data flows between the participants representing different teams. During this discussion, several new elements were added to the drawing.

Facilitator then asked the drawer to highlight those elements the R&D team would consider important for the workshop scope, and to explain how the proposed change would impact those elements. The facilitator continued by asking questions from the other participants about the impacts of the change. Whenever any potential impacts to other teams or systems, or any additional information needed or already available was identified during the discussions, they were recorded in the notes. This discussion, accompanied by drawing, went on for nearly an hour, until the diagram was considered adequate and the participants felt they had understood the scope (meaning the proposed change).

Threat modeling started with a recap of STRIDE model, and the facilitator asked each of the participants to provide their suggestions and viewpoints on each types of threats. In practice discussion mainly went on between two participants: the drafter and the representative of one of the solution teams, with only short remarks from few other participants. During the discussion, the details of the data flow diagram were further clarified, potential threats identified were listed on the notes,

and a new potential area requiring threat modeling was identified and recorded. Facilitator was moderating the discussion; whenever they seemed to feel that the discussion would go into too many details, or started drifting towards future plans that he considered irrelevant regarding for the scope of the workshop, they steered the discussion back to the current setup and workshop scope. They also frequently recapped what had been discussed between the two most active participants and asked for feedback and comments from the other participants, while they remained silent.

After the last STRIDE element, elevation of privilege, had been discussed, there was only few minutes of time left. Facilitator used this time to ask for additional input to be added to the notes and to thank the participants. They concluded that the recorded notes would be converted into new work tickets, including a new threat modeling workshop regarding another area identified during the workshop, and a follow-up meeting between the initiating R&D team and the third-party solution team. It was agreed that the owner would share the notes and that the data flow diagram via the threat modeling work ticket. The workshop ended at the planned timing. Case 2 workshop phases and participation are described in Figure 17.

Workshop phase	Introduction	Creation of data flow diagram	Threat identification	Workshop summary and closing	**Total**
Duration of the phase	15’	44’	45’	4’	108’
Active participants	• Facilitator • Owner (R&D team lead)	• Facilitator • R&D team member (the drawer) • Third-party solution 1 team member • R&D team member • Third-party solution 2 team member • Head of third-party solution teams • Owner (R&D team lead)	• Facilitator • R&D team member (the drawer) • Third-party solution 1 team member • Third-party solution 2 team member • Third-party solution 2 team member • Owner (R&D team lead)	• Facilitator • Owner (R&D team lead) • R&D team member (the drawer)	8 active participants (total 20 participants, excluding the facilitator)

Figure 17. Case 2 workshop phases and participant activity.

Case 2 post-workshop activities

The outcomes included several levels of work: the work that the initiating team could proceed with, planning work for other teams involved in the proposed change, as well as validation work regarding some of the elements owned by a team that was not present in the workshop. It was noted by the facilitator that the proposed change,

even though its implementation would be team-specific, was also relevant to many other teams within the organization. The owner mentioned they would start working on mitigating the identified issues with their own team by converting the notes to work tickets, and that they would also start contacting the representatives of the other teams who needed to be involved. The facilitator was planning to support the work tasks and to follow the progress, both because the work tasks involved several teams as well as because they considered the progress to be relevant for a wider audience than only the team who had initiated the workshop.

5.6.3 Case 3 description

Case 3 was a threat modeling session that had been initiated by a project team developing a software product to be sold to the organization's clients. The project team had introduced their product to the market approximately six months before. The project team in question had been conducting threat modeling activities together with the facilitators, and they had also arranged some privacy and security assessments for their product. As they had had several threat modeling sessions already earlier, they had been proactively identifying needs for these as the development work had proceeded.

The threat modeling in question was needed as the project team was about to add some new functionalities to the product, and they wanted to understand whether there were any threats that would arise from these changes. The team belonged to a larger business unit, which had its own quality function. The team had created a ticket for threat modeling work, and then they had contacted the quality lead, who then had initiated the threat modeling workshop with the facilitators.

Case 3 preparations for the workshop

The scope of the session, even though it was described as quite narrow, included a functionality that was considered important to be analyzed, as it involved important data as well as third party interfaces. This was the first time for the team as well as the facilitator to threat model this type of a setup (involving certain specific interfaces), and due to this, the facilitator had prepared for this by studying cases of similar implementations from different sources. Despite this, neither the facilitator

nor the quality lead expected any major findings, because the product in question was relatively new and developed carefully from the beginning.

The original thought of the team had been to threat model two implementations of the new functionality within one workshop. However, the facilitator had paid attention to this and concluded that the scope would be too confusing and the group too large to enable active discussion that would be required for the analysis in the given timeframe. They had agreed with the owner and the project manager that, in case needed, another workshop will be arranged for this purpose, and that this workshop would only involve the team members required for threat modeling this particular implementation, and project manager removed the participants working on the other implementation from the invitation list.

The planned duration for the session was 90 minutes, and the list of invitees consisted of development team members, project manager, lead architect and product program manager. The project managers and lead architect owned the actual work that the team would do, while quality lead was considered as the owner of the threat modeling workshop. Besides the objective of identifying the potential threats for the new functionalities, another objective was also to share knowledge about the product architecture to the development team.

Regarding the participants, facilitator and owner told that the lead architect and product manager had participated several threat modeling sessions also previously, and that also some of the other participants had previous experience. The owner also had a long experience in threat modeling and mentioned that threat modeling strongly supports their work daily work as quality lead. They described this as an optimal timing for the session, as the functionality that was planned to be analyzed was still been built but not finalized, and that the architecture was stable enough not to change in a way that would make threat modeling irrelevant.

It had been agreed prior to the workshop that the lead architect would be responsible for drawing the data flow diagram during the session. An initial plan was also that the project manager would be the best person to take notes, as they would be responsible for managing the project backlog that would include all the work tickets created after the session.

Case 3 threat modeling workshop

The workshop was held with a help of an online meeting tool that included a possibility for audio, video, screen sharing and chat. Besides the owner, the workshop participants included the lead architect, project manager, project portfolio manager and project team members. Lead architect, who was acting as a drafter, had a camera and whiteboard setup at their office, while the facilitator had a similar setup at their premises for backup.

The workshop started by introductions and going through the roles. As the project manager was not able to take notes for practical reasons, it was agreed that the owner (quality lead) would act as the note taker. Facilitator then showed two whiteboard drawings with their camera: an example of a data flow diagram and the definitions for the elements of STRIDE model. They first presented what the data flow diagram would include and explained its purpose in threat modeling, and then also introduced the STRIDE model, its elements, and that there was also a chance that some other types of threats would be identified. They also briefly mentioned another model, TRIM, which would suit for the cases that include a lot of personal data.

The drafter (lead architect) explained two scenarios that were planned to be discussed during the workshop. Facilitator suggested starting with one of the scenarios, and the discussions commenced. The drafter started drawing the flow for the scenario by drawing the process transactions between the system elements as well as the data that is transferred through the process between the elements. They also explained which of the elements and were not controlled by the product team or even the organization and asked some clarifying questions from the other participants while drawing. Only one other participant as well as the facilitator commented during the drawing. The facilitator also asked clarifying questions which were mainly answered by the drafter and the only active participant. Even though the facilitator and the owner both reminded the participants to ask questions and give comments, and tried activating them, they remained silent despite of the one active participant. During the drawing, the facilitator also explained some details regarding the trust boundaries, switching to their whiteboard, and then the same details were added to the main drawing created by the drafter. Finally, as the

drawing was agreed to be ready between the active participants, the facilitator suggested the drafter to go through the whole diagram once more. The facilitator still asked some clarifying questions, and the drafter added new elements based on those.

After this, it was time to move on to threat modeling. Facilitator started this by asking questions about the flow that crossed many boundaries. The drafter and two participants were involved in the discussions. As the discussions proceeded, the facilitator and the drafter continued identifying threats and the owner assumed the role of asking clarifying questions to ensure they could capture everything in their notes. Certain things that were discussed were concluded not to be that relevant whereas some were listed as findings. The discussions varied from analyzing technical details to evaluating roles and responsibilities, and the facilitator once and a while commented on which elements of the STRIDE model had been covered. The discussions resulted mainly notes regarding the team's own responsibility area but also an action to check from the stakeholders how some of the interfaces were built and secured.

When the workshop was ending, the owner read through the notes they had made during the session, and the facilitator asked for feedback on whether everything had been covered. The owner then explained how they would be sharing the notes, and the drafter took a picture of the data flow diagram to be added to the work ticket together with the notes. Project manager suggested a retrospective to be conducted of the session between themselves, the owner, and the facilitator, and this was also noted. Case 3 workshop phases and participation are described in Figure 18.

Workshop phase	Introduction	Creation of data flow diagram	Threat identification	Workshop summary and closing	**Total**
Duration of the phase	15'	32'	32'	6'	85'
Active participants	• Facilitator • Owner (quality lead) • Project manager • Lead architect (the drawer)	• Facilitator • Lead architect (the drawer) • Project team member 1 • Owner (quality lead)	• Facilitator • Lead architect (the drawer) • Project team member 1 • Project team member 2 • Owner (quality lead)	• Facilitator • Owner (quality lead) • Project manager	5 active participants (total 9 participants, excluding the facilitator)

Figure 18. Case 3 workshop phases and participant activity.

Case 3 post-workshop activities

The owner, project manager and facilitator had conducted the retrospective to discuss the meeting benefits and challenges. Regarding the technological arrangements and the outcome, the workshop was considered to have met the expectations. Based on this, they had decided that the threat modeling already planned for the other implementation was no longer needed as the workshop outcomes would also cover that scope.

They had also concluded that the workshop had served as a good first experience in arranging a threat modeling workshop online. On the other hand, the interaction during the workshop had not gone as expected, as so many of the participants were silent throughout the workshop. The owner also mentioned that – due to the session being arranged online – it was very difficult to say whether the more silent participants were benefitting from participating the workshop, as their reactions could not be observed. As a development idea, they had planned to organize the next workshop with a smaller group, and then to organize a short walkthrough for the rest of the team afterwards for information sharing purposes. Another development idea was that project manager could support the discussion by asking questions from the other participants, as they know their competencies and where they could best contribute.

As the owner had made the notes but the project manager was the one who was at the end responsible for converting the into work tasks, the owner planned to contact the project manager already on the next day to support this. They thought this would be beneficial for them both, as the owner would see that this is done, and the project manager would need to think about the notes from the work ticket perspective. Most of the tasks were in the form of questions to some other team, and based on these clarifications and validations, the actual security improvement work would then be planned. There was a need to identify whether this specific part of the process could be done in another way, and the team cannot evaluate this by themselves.

As the topic was also new to the facilitator, they intended to follow-up the progress of the tickets to learn more on how the team decides to proceed. This would help them in facilitating workshops with the same scope to other teams as well.

6. Results and key findings

The previous Chapter 5 describes the empirical research approach and the three cases analyzed for this study. This chapter describes the results and key findings based on the research material.

As discussed in section 5.4 of Chapter 5, the actual analysis consisted of two phases: first, the results were organized based on key themes emerging from the research material, and second, these organized results as well as the original research material were sensitized with theoretical concepts related to knowledge, knowledge creation and social capital discussed in Chapters 2, 3, and 4 to identify key findings and related theories and concepts explaining knowledge creation in threat modeling workshops. Section 6.1 of this chapter presents the results based on the themes emerging from the material, and section 6.2. then focuses on key findings and those theories and concepts that would fit best to explain them.

As part of the results, some direct quotes from the interviews are used for demonstrating how the topics were discussed within the workshop and in the interviews. All the interviewees and workshop participants are referred to as “they”, independent of their gender identity. Quotes from Finnish interviews have been translated into English.

6.1 Themed results

The first phase of the data analysis included reading through the material and identifying key themes that seemed to have an impact on knowledge creation in each threat modeling workshop. The emerging themes included 1) documents and models; 2) participants; 3) facilitation; and 4) scope. Next, the material was grouped under these themes. This led to adding sub-themes under the themes as described in Figure 19:

Documents and models	Participants	Facilitation	Scope
• Data Flow Diagrams • STRIDE model • Workshop notes • Storing the documents	• Reasons to participate • Contribution activity	• Facilitation during the workshops • Facilitator's own knowledge	• Impact of cross-boundary interfaces • Impact of "legacy" • Identifying the needed knowledge

Figure 19. Themes and sub-themes emerging from empirical research material.

This section will discuss the results categorized in these themes and sub-themes, as well as describes the observations related to each category.

6.1.1 The role of documents and models

All the interviewees stressed that a suitable knowledge for threat modeling the intended scope did not exist and that a common understanding needed to be formed first before being able to start identifying threats. Even if there would have been such documentation, it would not have been considered to be a good approach to use that as a basis for the modeling, especially if the details required for modeling threats were different from what had been included in the existing documentation:

"<…> This kind of a big chunk that gets people depressed. There have been some sessions that have been based on an existing interaction diagram or flow with approximately 700 arrows, and it creates this kind of a reaction. It kind of invites participants to run through the whole thing very quickly because there is a limited amount of time. Another thing is that the visualization has an important meaning particularly in this kind of a situation where it is essential to understand the interaction between different elements, and in what order the messages flow happen, and what the messages contain, and this means one needs to discuss these on very detailed level. If you have some existing architectural diagram, it will include so many details that it would be impossible to manage going through them all." (Interviews)

The interviewees mentioned, e.g., architectural drawings, data flow diagrams and message sequence charts as potential types of diagrams to be used for drawing a description on the scope. In all the three cases, a data flow diagram was drawn.

Data flow diagrams

The first step in the workshops was to form an understanding of how the system(s) in scope worked in practice. During all the three workshops, data flow diagrams were used for this purpose. In all three cases, data flow diagrams included the main systems/elements and data flows within the intended scope of the workshop, the related trust boundaries, inputs and outputs, and storages. Drawings were detailed based on the needs in each workshop. A generic example of a data flow diagram is included in Appendix 3.

Independent of their knowledge and role regarding the scope, the persons drawing the diagrams were not able to create it purely by themselves but relied on the support from other participants as well as the facilitator to include all the relevant elements.

<…> Participant E wanted to add some details into the diagram, and drafter added these into the drawing. Drafter and participant C continued detailing the diagram <…> (Workshop observations)

Systems/elements that created the most discussions in all three cases were the ones which had a “cross-boundary” nature: for example the interface between two elements was locating either between systems or between responsibility areas, and both the input and output data needed to be thoroughly understood. These cross-boundary situations also generated most of the needs to further clarify something after the workshop. In those cases, the note taker recorded this need into the workshop notes to do the “clarification” with either the team or the solution provider being responsible for the system/element.

Data flow diagrams were also used to go through the threat scenarios during the actual threat identification phase, which followed the modeling phase. As it had been done when creating the data flow diagrams, also this work utilized the who does what approach, and focused on understanding how the potential threat could realize when human actors would be involved. The identified threats were linked to the relevant parts of the diagrams.

STRIDE model

The STRIDE model (described in Appendix 4) also had an important role in threat identification. Based on the interviews and workshop observation, using STRIDE supported knowledge creation in a sense of providing common terminology for discussing different types of threats. It was introduced at the beginning of all the three workshops, and its elements were also explained. All the workshops also involved both participants that were used to working with the model to go through potential threats and participants who were new with the model.

Another function for STRIDE was that it acted as a reminder to go through (at least) all the threat types discussed in the model. In all the workshops, the threats identified followed the structure of STRIDE model. However, the facilitators emphasized that it should be used rather as a guidance/reminder than a structure, and applied based on the context:

"It should not be used for categorizing the findings but rather as a reminder to go through at least all the six areas it covers. <…> I always think what would be the better way for the participants but on the other hand the creative thinking or the investigative testing can suffer if you limit the discussion too much, for example if you say that hey let's think about this spoofing threat. It's not that important to know what type of a threat it is, it's important just to go through all kinds of threats and also remember to go through different types of threats." (Interviews)

Both the creation of the data flow diagrams, and threat identification done with the help of STRIDE model strongly utilized a viewpoint of a human actor interacting with the system. The facilitators described these narratives as "use cases" (for data flow diagrams) or "threat scenarios" (for threat modeling), meaning that for data flow diagrams, the actor was considered someone using or maintaining the system, whereas when using STRIDE, the actor was considered someone who would attempt to misuse the system.

"The main thing in drawing the data flow diagram is to do it from an angle of someone doing something within the system – it should not be only a drawing about architectural building blocks, which is easily the case if this angle is not understood." (Interviews)

The work done with data flow diagrams was described in one of the workshop discussions as *“validating the assumption whether some other team is doing something or to make sure things work as they are supposed to work” (Workshop observations).*

Workshop notes

Besides the diagram, also text documentation was created during the workshops. The note taker was writing down the identified threats as well as those parts of the discussion that were found essential for planning the work. In all three cases, the owner acted as a note taker. The approach for the drawings and the notes was a bit different: the drawings were visible throughout the workshop for all the participants, whereas the notes were shared after the workshop. In case 3, the owner also went through the notes at the end of the workshop with other participants, and in all three cases, participants were encouraged to suggest additions or amendments on the shared notes in case they would notice anything.

All the interviewees emphasized the importance of the notes as part of the documentation created in the workshops, as the notes would support in planning the work after the workshop. The facilitators stated that the person who would be responsible for planning and prioritizing the work in the backlogs would be ideal for the note taking role, as they would possess the best understanding on how the findings from the session would link to the team’s daily work.

Storing the documents

The diagrams including the identified sources of threats were included in the threat modeling workshop’s work ticket after the session together with the workshop minutes and notes. The purpose for this was stated to be to have them available later when the teams would be progressing with threat modeling related work.

“Data flow diagram is useful also later in case there is a need to clarify something related to the architecture, and it should be drawn into electronic format in case it seems it is useful. I have used them in discussing the tickets created based on threat modeling and how they have been proceeding, because it is a good way to remind of what was discussed during the workshop.” (Interviews)

In all the three cases, only a part of the whole discussion that underwent during the workshop was captured in the drawing or the notes. It was also brought up in the interviews that the documentation alone would not provide all the aspects needed for threat modeling:

"If the workshop does not manage to go through the whole scope, it would be much more difficult to continue later without first going back to the scope and the flow. People just tend to forget details that have been discussed, and they do not anymore have the same understanding if the modeling continues later." (Interviews)

6.1.2 The role of workshop participants

Threat modeling workshops analyzed for this study had three main workshop roles: one participant had the main responsibility for the drawing, one participant (which regarding all the cases happened to be the owner) was responsible for recording the findings and creating the minutes and notes, and the facilitator was responsible for steering the overall flow and the progress of the discussion in order the objectives to be reached. Rest of the participants were expected to contribute into the discussion and thereby help in creating the understanding on how the systems in scope worked and what the potential threats could be.

In all three cases, threat modeling workshops were held online, and a group of people joined these workshops for a pre-defined time and worked – or at least were expected to work – together to identify threats within the selected scope. The objective to identify threats within the selected scope set some expectations for the participants for joining the workshop.

In the actual workshops, the participants had two main modes of action: they either participated in the discussion actively, or they stayed silent throughout the workshop. Additionally, in cases 2 and 3, some of the participants commented when specifically addressed by the facilitator or another participant. Independent of their level of activity, all the participants were included in the workshop minutes as equal participants.

Reasons to participate

Regarding reasons getting engaged in threat modeling related knowledge creation, the owners seemed to purely consider it to provide useful insight on what kind of threats the scope could include, and thereby to enable them to identify what kind of actions would be relevant regarding these threats. Case 2 and 3 owners also referred to their organization's existing security policies which also included instructions and expectations for threat modeling, and that it had some impact on when and how they threat modeled. The facilitators as well as the owner of case 3 who worked with development teams also mentioned that threat modeling at the early stage of development would save a lot of time and effort, as it would help identify and mitigate threats when it would be still easy to change the approach in order to do this.

The intended participants got the information about the upcoming threat modeling workshop from the owner or some other person who had been initiating the session. This information contained the scope and objectives of the workshop as well as some preparation instructions and a calendar reservation. In all cases, threat modeling had been discussed in person with the originally invited participants before the workshop. In case 1 and case 3 workshop, all the participants belonged to the same team, whereas case 2 setup was slightly different, as it included participants from different teams.

As part of case 2 workshop preparations, the facilitator had contacted a few people when identifying the additional knowledge needed, and as it was found important that they would participate, they were invited, and when the session came closer, the facilitator had also ensured those invitees would join the session. In cases 1 and 3 the owner and the teams had discussed the scope and objectives of the workshop together before it took place.

Regarding case 3, the facilitator commented in pre-workshop interview that the number of participants was maybe too high considering the scope of the workshop. The owner of this workshop also considered this a possibility for the invitees to get some new information:

“These sessions are also good for sharing knowledge, as it is very rare that the lead architect will go through their plans in such a level of detail. I hope that all the developers would understand the details better after this session, meaning that they know that something is done in a certain way because of this reason.” (Interviews)

All the originally invited participants joined the workshops except for one person invited for the workshop of case 2. In case 2, the person who did not join the workshop had forwarded the invitation to some of their team members.

Contribution activity

The facilitators emphasized that a workshop would include the suitable set of participants, when all individuals participating would be able to contribute into the discussions. Rate of the active participants vs all participants in case 1 was 100% whereas in case 2 it was 40% and case 3, 56%. Participation activity throughout each workshop is described in more detail in Figures 16, 17 and 18.

In case 1, both the owner and the facilitator were content with the level of activity of the participants, and they also considered they had all the right participants in place in terms of what kind of contribution they needed:

“<…> there were not that many things where we didn’t have any answers to. We only had like one thing during the session that the team wasn’t able to answer. Another thing was that the participation was very active, and people were asking questions and there was somebody who was willing to draw. Nobody was just waiting for somebody else to do things. So I think this team had adequate knowledge as well as the seniority in order to make the session active. Participants were very enthusiastic to participate.” (Interviews)

In cases 2 and 3, quite significant number of participants did not contribute at all. Regarding case 2, most of the participants who stayed silent were the ones invited by the original participant who was not able to join the session.

For case 3, the owner stated in the pre-workshop interview that a secondary objective for the session was also to share knowledge, as it included a thorough walkthrough of the architecture and data flows of the functionality in scope, which was valuable knowledge also for those team members whose daily work was to

develop a smaller part of the system. After the workshop, the owner mentioned they were not sure whether this had happened:

"Generally speaking, the sessions are also of informative nature and the intention is to share with the development teams the reasoning behind certain solutions and things that they need to consider when they are doing the development. I think there was some information sharing but it's very difficult to be sure about this because in a live session you can see for example when people nod as an agreement or in case there are people who are not focusing. You just can't tell so there is an uncertainty about this <whether the information sharing did take place>." (Interviews)

In the post-workshop interview the owner mentioned that they had been discussing this with the facilitator, and decided that for the future workshops, the invitees would only include such participants who would be needed for threat modeling work.

From both the facilitator and owner point of view, the high number of non-active participants seemed to be a slight concern. Regarding case 3, it was concluded by the facilitator and the owner that the lack of activity of the silent participants was due to their objective of acquiring knowledge rather than participating in the discussions. On more general level, the facilitators also identified some other reasons for potential non-activity of the participants:

"There can be various reasons <why someone does not actively participate>. It can be because of the attitude, having already an existing opinion about the topic and feeling that a two-hour session would be a waste of time. This can also be a question of personality, or it can be happening due to group dynamics. For example, in R&D work the scope often includes work done by that specific team, and sometimes there might be some senior team members who are rather dominant from social perspective. The others may be afraid to question or challenge their opinions, especially when there are external people present in the session. Some teams and cultures are more hierarchical than other." (Interviews)

Both the facilitators and the owners brought up the workshop arrangements when discussing the participant activity and the high rate of non-active participants in cases 2 and 3. As threat modeling workshops had traditionally been arranged as

onsite workshops, it was discussed whether arranging the workshop online would have impacted in the activity of the participants. However, this was not considered as the main reason for non-activity. Instead, it was concluded for case 2 that the online workshop might have been an underlying reason for the unexpectedly high number of participants – it was felt the online format of the workshop gave the silent participants a better chance of remaining silent, and as the number of participants was higher than planned, the facilitator or the owner were not able to offer enough support (e.g., to address them with suitable questions) in order to ensure everyone would participate.

6.1.3 The role of facilitation

In all three cases, the owners as well as most of the workshop participants had previous experience in threat modeling activities: in case 1, the team had done threat identification as part of their daily work. This was also mentioned in cases 2 and 3 but according to the owners, the teams involved in initiating those cases had also been running regular threat modeling workshops. The owner, representing the initiating team of case 2 threat modeling work, mentioned that they had been doing threat modeling both with and without external facilitation, and for those workshops where an external facilitator had not been involved, the owner, who was also the team lead, had been acting as facilitator. Case 3 team had only been running threat modeling workshops with a help of an external facilitator but some of the team members also had experience in threat modeling without an external facilitator.

The facilitators had been working with various teams and team combinations. They mentioned that the role of an external facilitator was strongly linked to the context as well as the experience of team initiating the threat modeling work. The level of experience of the initiating team was considered to impact also on the role of the facilitator during the workshop:

“<…> people involved in this kind of sessions are a bit different anyways: when threat modeling with an R&D team, they have been responsible for developing the solution, whereas regarding SaaS solutions it sometimes may be that the participants do not have that much of an R&D or even IT background, and this requires a very different approach. But eventually the same questions arise, for

example how to do the modeling, even though the level of abstraction would be different." (Interviews)

"Some teams know the potential challenges within their technologies very thoroughly and they are capable of doing threat modeling on daily basis by themselves. In case I join such sessions, my role is purely to facilitate, and I will help them clarify things or support the overall dynamics by making sure everyone contributes and potential disputes are solved. Then on the other hand, there are teams having such limited competences that I have felt I have been doing threat modeling and even the drawings all by myself. It can be for example that the team has been focusing so much on for example producing the code that they simply do not understand the bigger picture and the relationships between what they are doing and the other teams and systems." (Interviews)

Regarding the impact of the context, a cross-team scope was considered to be such a context where an external facilitation would be the most useful: in those cases the facilitator would not be representing any of the teams participating the workshop and would be able to purely act as a moderator for the discussion.

Facilitation during the workshops

All the three cases involved an external facilitator. After the initiating team had contacted the facilitator and it had been agreed they would be involved, the facilitator and the owner had started planning the workshop by going through the scope and objectives for the modeling. Based on these discussions they had also selected suitable participants to be invited in the workshop and had also formed an initial understanding of the previous threat modeling experience of the participants.

At the beginning of the workshops, the facilitators ran through short introductions, as well as explained the scope and the objectives of the workshop. They also emphasized the open discussion needed for threat identification, and explained the ways of working that were planned to be used. This part, at its minimum, consisted of a presentation of the approach, tools and methods that were planned to be used in the workshop in question, as well as an introduction to the roles of the drafter (person having the main drawing responsibility), the note taker and the facilitators. As all the workshops used data flow diagrams as tools for describing the scope, and

STRIDE model as a support for identifying the threats, both were explained to the participants. In all three cases, the facilitators also mentioned TRIM, an alternative model that would suit for threat modeling in cases where there is a lot of personal data involved.

In cases 1 and 2, it had also been agreed with the owners that the introduction would consist of a wider introduction to threat modeling. This introduction, supported by a PowerPoint presentation, begun with a walkthrough of reasons for threat modeling, continued with a wider set of examples of modeling tools and diagrams as well as analysis models (besides STRIDE and TRIM), an introduction to potential cognitive bias that could prevent threat identification, and some detailed instructions on how to continue the work after the workshop. In case 1, the facilitator also participated in the discussion about what would be the proper scope for the workshop as part of the introduction (see case 1 description in Chapter 5 for further details).

The first phase of threat modeling included drawing the data flow diagram. During this phase, the facilitators kept up the discussions by asking both general level and more detailed questions about the data flow and the elements. The questions were addressed to all the participants, as well as directly to individual participants. They also checked once and awhile whether there were any questions about the diagram or whether anyone had any comments. At the stage where the diagram started to look being close to finalization, they asked the drawer to walk through the diagram for the participants, and during and after this still ensured whether anyone had anything to add before moving to threat identification.

During threat identification, facilitators continued to support the discussion with generic questions:

Facilitator supported the discussion by asking questions such as: ”If I do this, am I able to do that?” They also encouraged participants A and B to bring in their insight. Participant B contributed with an example that was not a spoofing but tampering related threat, and participants C and D also discussed whether this was possible. (Workshop observations)

During the discussions, the facilitators also often posed more detailed technical questions:

Facilitator then asked the team to describe one certain functionality of the system and how this was built within the system. Participant A said that participants C and D were probably able to answer this question. Facilitator then asked them to explain how the system was built to prevent spoofing, and participant A commented that <technical details>. Facilitator then continued by asking more questions, especially about the flows crossing the trust boundaries, and participant A answered those. The discussion moved into technical details and went on mainly between facilitator and participant A. (Workshop observations)

The facilitators also ensured the timing of the workshop and tried to involve as many participants as possible by asking both open and directed questions. They also repeated several times that the focus should be in identifying threats and not trying to find solutions or to discuss technical details regarding on how the mitigation should be done.

Towards the end of each threat modeling workshop, the facilitators went through with the owners on what would happen after the workshop regarding the notes and documentation, and ensured the owner took the responsibility for continuing the work. In all three cases, the facilitators and the owners also had a separate walkthrough of the workshop and its outcomes after the actual workshop. The facilitators stressed that they do not usually get involved in converting the notes into work tasks. In cases 1 and 2, however, the facilitator promised to support the owner in this, and also for case 3, the facilitator planned to follow through on how the work would progress (see related case descriptions in Chapter 5 for further details).

Facilitator's own knowledge

Both the facilitators and the owners highlighted that the role of the facilitator included "keeping the pace", involving the participants and steering the discussion in a way that the workshop would reach the desired outcomes. In case of potential disputes, the facilitator would ensure that they would be solved.

"I think <…> was very precise and thorough and asked clarifications until everything was understood. <…> also is very good in using small things to control the clarity of the session for example going through some part of the drawing once again just to

make sure that everybody agrees and understands or repeating what has been written." (Interviews)

The owners also brought up that the facilitators had a deeper understanding of potential threats than the participants did, and they considered this knowledge very valuable from the participants' point of view. Examples of such knowledge were also being noted during the workshop observations.

Facilitator commented that especially <technical details> would propose a threat in case this would be used, and that it would be good to check whether any of the interfaces would use this. Facilitator also suggested having a further discussion about this before deciding on the actions. (Workshop observations)

However, the facilitators emphasized several times that they would not prefer to be in a role where they would identify threats on behalf of the participants but rather ask questions and steer the participants to identify the issues and threats themselves as they wanted to assume *"team themselves also have deep knowledge on the topic" (Interviews).* Facilitator for case 3 workshop also mentioned some means that the participants could use to acquire knowledge of potential threats to increase their knowledge from this angle:

"<…> I think this is the generic level knowledge one needs. The things that OWASP Top 10 reflects, or SANS 25." (Interviews)

On the other hand, the facilitators stated that having some prior knowledge on the technologies or systems in scope would help to ensure at least most of the potential threats would be identified during the workshops. They also explained that in case they considered themselves not to have adequate level of knowledge on the technologies or systems in scope, they would at least try to learn the basics about them before the workshop. They also mentioned that certain technologies and the related threats would develop so fast that it would require additional effort to maintain the related capabilities and knowledge:

"<…> there are some technologies like <technical details> that develop so fast that even if you have facilitated a session six months ago, the knowledge you got from that session about the potential threats is no longer relevant." (Interviews)

Facilitators thought they also benefitted from each other's experience and knowledge:

"We <facilitators> have learned a lot from each other during our co-operation, and sometimes we go into each other's sessions just to learn from each other. We have slightly different experience. <…> we still do joint sessions sometimes and we also share knowledge between each other and look at each other's findings from the system." (Interviews)

6.1.4 The role of scope

Based on the interviews, many preparation activities had taken place before the workshop, including the initiation of threat modeling (and creating the related work ticket), discussing the intended scope, objectives and needed participants with the facilitator and the initiators, agreeing on the scope, objectives and participants, identifying and sharing potentially relevant existing documentation, and pre-informing the rest of the participants from all of these.

Defining the scope for threat modeling was considered an important part of the preparations, as it was seen to be linked directly on what kind of knowledge is needed for being able to get a holistic understanding of the systems/functionalities in scope, how they are built, and how they interact. Scope was seen adequate when it was not too complex, and it is possible to do the analysis within time reserved for the workshop. Duration of case workshops varied between 90 to 120 minutes, which according to the interviewees was an optimal duration of a threat modeling workshop from the efficiency viewpoint.

Two factors impacting the complexity of the scope were repeating in the interviews: the number of element/system external interfaces and related transactions that go across boundaries, and the legacy of the system that formed the scope. These factors were also considered to have a significant impact on knowledge needed for threat modeling.

Impact of cross-boundary interfaces

Especially the facilitators saw the interfaces between different boundaries (for example system or responsibility boundaries) to be important from threat modeling point of view:

"Software can fail on many levels. It is not only that a line of code includes some defects, but things also can go wrong because the team assumes some other team does something in a certain way." (Interviews)

The significance of boundaries in defining the scope and adding complexity was highlighted especially in case 2 where the workshop was initiated by an R&D team that was using system-related services provided by two other teams, and they wanted to make a change that required changes in those two systems. Even though they had an initial suggestion on how the new interface should have been built, they were not able to identify the potential threats related to this change without involving the representatives of the two other teams. The owner had originally thought about inviting a much smaller number of participants to the workshop to analyze the suggestion for building the interface but after a pre-analysis had been done with the facilitator, it was decided to first analyze the current setup that connected the systems between the three teams. This analysis resulted in findings that showed it was indeed useful to do the analysis involving a wider set of participants from different teams.

According to the facilitators, understanding the boundaries is also important because of their nature, as they can often contain significant threats:

"One way to identify important findings during the sessions are the trust boundaries. I mean that when things cross the boundaries. I've seen so many things going wrong when people are doing threat modeling and discussing how different elements talk to each other when they are within the same process and it actually doesn't matter. I think it's important to make people understand that you need to think about data input and output across trust boundaries and then after that there needs to be some understanding on what can go wrong when handling inputs and outputs." (Interviews)

Case 1 involved a SaaS service that was run by a solution provider and not the organization in question, and naturally this interface was also considered as a boundary interface. The facilitator and the owner emphasized that threat modeling in this case meant focusing mainly on those elements the organization was able to impact themselves:

"It is so that "backend is a black box" in this case. We need to understand that some of the information we might need is such information that we are not going to have, meaning that we have to live with those descriptions and reassurance they <the solution provider> are willing to give us. This is usually ok but it has to be kept in mind that we may never be able to know on a detailed level how some solution provider operates their platform, and of course it is not our business anyways as we are their customers and we trust whatever the service agreement says." (Interviews)

Impact of "legacy"

Another factor considered to have an impact on the complexity of the scope was "the legacy" the system would include, meaning the exact knowledge on how it had been developing throughout time into its current state did not exist. This was considered to be one of the reasons for case 3 workshop being a relatively "simple" one; case 3 was initiated by a project team that were developing a relatively new product that was considered to be built more or less on a "clear table", which had been threat modelled continuously on different levels as part of the development work, and the development of which was completely managed with a help of work management system. The facilitator commented the difference to older products as follows:

"If you do this retroactively, if you threat model something that has been sort of growing throughout the years and where this and that has been added, even though the original plan and architecture would have been good but some drifting has happened throughout time, in those cases, you usually just find more <threats>." (Interviews)

The meaning of legacy embedded in the systems was also seen to add complexity to threat modeling done for organization-wide technology solutions:

“When we look at group-level IT solutions instead of what we have developed ourselves or tools we use for certain purpose only, it requires a very different level of understanding on the enterprise architecture and its – sometimes even quite peculiar – characteristics. And of course, solutions that have existed for longer time may consist of various instances and sub-elements that also may be at different phases in their lifecycle. If you want to threat model this kind of an entity, you have to understand things that may be for example 15 years old as well as things that have just recently been implemented, and this can be quite challenging.” (Interviews)

Case 1 scope included an organization-wide solution, and even though the scope of this workshop was pre-planned between the owner and the facilitator, it still shifted at the beginning of the workshop, focusing on a sub-element that was easier to be understood and analyzed within the planned time frame.

Identifying the needed knowledge

Scoping and the following preparations also included identifying the potentially useful existing information and documentation. It was mentioned several times in both the interviews and during the workshops that no existing documentation would have likely served the exact purpose for threat modeling in any of the cases but that this kind of integrated documentation was expected to be created during the workshop. Existing knowledge was used mainly for preparing for the workshop, whereas the knowledge needed for threat modeling was created in collaboration between the participants at the workshop. This setup assumed the access to parties with the knowledge should be in place during the time window planned for the workshop.

The facilitators and the owners had had thorough discussions on who would possess adequate knowledge for the elements in scope, and they had identified the potential workshop participants based on these discussions. In case 3 preparations, it had also occurred that the scope included elements the team had not worked with before, and the facilitator did not have experience on those elements either. The facilitator solved this dilemma by self-studying about the elements prior to the

workshop so that there would be at least one person capable of threat modeling this part of the scope.

Although the facilitators and owners worked together on many levels and ways to ensure the workshop would result in identifying all the relevant threats for the scope in question, threat modeling itself was described to be a “never-ending circle”:

“The more you do, the more you know. The more you know, the more you need to do.” (Interviews)

“It is impossible to make sure everything is discussed and analyzed. I could compare this with testing: when you do testing, you cannot prove there are no bugs, you can only prove there are bugs. In testing, you cannot claim that you have found all the bugs. Nobody in their right mind would say that.” (Interviews)

6.2 Key findings

After the initial findings were categorized in themes, they were also compared with the theories and concepts evaluated as part of the literature review (Chapters 2, 3 and 4). In this analysis, some additional aspects emerged from the perspective of social capital and its impact on knowledge creation. As part of this analysis, the set of theories and concepts discussed in Chapters 2, 3, and 4 was further clarified. The initial observations from the empirical research were then reflected with the set of theories and concepts resulting from these iterations to identify mutual connections. Next sections describe the connections that were identified in this reflection.

6.2.1 Knowledge creation

Knowledge creation takes place within a continuous interaction between individuals or individual and their environment, and it always involves both exchanging and combining knowledge. As a result of this continuous knowledge creation, knowledge and its context are constantly changing. Knowledge exchange can take place through socialization, where tacit individual knowledge becomes tacit collective knowledge, and externalization, making tacit knowledge to explicit format. Knowledge combination assumes that knowledge in its explicit format is combined to form renewed explicit knowledge, but combination also takes place as internalization, when explicit knowledge becomes part of individual or collective tacit

knowledge. (Nonaka 1994; Nahapiet & Ghoshal 1998; Nonaka et al. 2000). Knowledge exchange and combination require four conditions to be in place: access to knowledge, anticipation of value, motivation, and combination capability. (Nahapiet & Ghoshal 1998), and elements of all these conditions were identifiable in the research material.

Access to knowledge

Based on the research material, any individual participating in the workshop was not alone able to form a thorough enough understanding on how the system would work or what the potential threats would within the selected scope. However, access to such knowledge was a key success factor for threat modeling; having proper access to knowledge helped the participating team(s) to start with threat mitigation activities after the workshop and not use time for additional clarifications or validations. To ensure adequate access to this knowledge, the facilitator and the owner pre-analyzed the scope and identified the desired participants for the workshop. It is also worth mentioning that – as Nahapiet & Ghoshal (1998) also state – access to knowledge itself does not enable knowledge creation. This was obvious regarding those participants who participated the workshop but did not contribute to the discussions.

Anticipated value and motivation

Anticipated value and motivation were observable in the workshops in the form of participation. Those participants who contributed into the discussion did so as they felt their contribution mattered for reaching either the collective objectives for the workshop, or maybe in some cases also potential individual objectives they had set for themselves. The anticipated value, however, seemed to differ between the participants, and this was also a likely reason why for some participants, the "motivation" to get engaged meant joining the workshop to get information about the system and the threats. In case 3, this secondary, knowledge sharing objective of the workshop was also clearly stated by the owner. This is again in line with Nahapiet & Ghoshal's (1998) findings on the importance of all four conditions existing before knowledge creation can take place. Facilitator and owner roles during the workshops included encouraging participation, which could have led into

increased activity but based on the research material, did not have an impact in the analyzed cases. A wider perspective to the anticipated value and motivation could be embedded in organizational policies, that were referred to in the interviews: these policies seem to create certain expectations for the individuals to do threat modeling in the first place, and also to join the workshops in case their knowledge is needed.

Combination capability

Threat modeling tools, approach, and facilitation in all three cases were used for creating a shared context and enhancing combination capability. STRIDE model provided the facilitator and the participants with a shared language (Nahapiet & Ghoshal 1998) to discuss the potential threats, whereas the data flow diagram also acted as a boundary object (Nahapiet & Ghoshal 1998, Fong 2003) but also as a sounding board during the discussions, as using it jointly and visibly throughout the workshop also showed the participants how the knowledge related to the scope was formed. The connection between the data flow diagram and the notes was complementary, as the diagram described the “movement” (which is the order/flow of the activities) and to some extent also a spatial view (which instances are involved at which stage) of the scope, and the notes then included technical details to fulfil this knowledge.

Shared context

Nonaka (1994, Nonaka et al. 2000) establish their process of organizational knowledge creation on an assumption that knowledge develops through socialization and combination that require a shared context. Blackler (1995) introduces aspects of shared context as part of the encultured knowledge, meaning the social transformation of knowledge that leads to shared, collective understandings. During the data analysis, the significance of shared context as part of knowledge creation in threat modeling workshops was highlighted through many observations.

The facilitation with the help of various clarifying questions supported creating common cognitive ground, and discussing the system with the help of use cases, and considering threats as scenarios where an actor would misuse the system acted as shared narratives, supporting the shared understanding (Nahapiet & Ghoshal

1998). Threat modeling workshop itself can be considered as one form of “ba” or “shared context in motion”, as it provided the participants with an access to a pre-defined knowledge during pre-agreed period of time and space in order to join their individual context to form a shared context and to create knowledge. (Nahapiet & Ghoshal 1998, Nonaka et al. 2000).

One key observation was the overall lack of shared understanding between the participants of the potential threats in all three cases, and in case 2, where the participants represented different teams, also of the threat modeling scope itself formed by different solutions. The workshops seemingly had an important role in forming a joint understanding of the scope and the related threats.

In all three cases, the facilitator appeared to have the highest expertise in threat identification, utilizing their already existing knowledge in suggesting potential threat scenarios. In a situation where the facilitator was the only one understanding the “big picture” of the scope as well (case 2), their responsibility besides taking the team through threat identification was larger and included also ensuring a proper data flow diagram was created. In cases 1 and 3 where both the facilitator and the owner (case 1) and lead architect (case 3) had a solid understanding of the scope, the facilitators seemed to focus more on threat identification. The facilitators aimed at increasing the knowledge (and knowledge overlap) on how to identify potential threats by explaining the threat modeling approach and tools at the beginning of each workshop, as they thought this would improve the participants’ possibilities to identify threats during the workshop but also as part of their daily work.

SECI model

SECI model describes the conversion of knowledge between its different formats. Knowledge conversion takes place on both individual and collective levels and between explicit and tacit modes simultaneously and as a continuum. (Cook & Brown 1999; Nonaka et al. 2000). Social interaction ensures the resources of exchange and combination (meaning the tacit and explicit knowledge) takes place (Nahapiet & Ghoshal, 1998). Continuous knowledge conversion was thereby observable only among the active participants who were seemingly participating in social interaction. The workshop itself as well as the STRIDE model were both

supporting the socialization of knowledge through shared meanings (Nonaka et al. 2000), and the role of data flow diagram as a boundary object (Fong 2003) was crucial in enabling the knowledge exchange. Observing the whole spiral of knowledge conversion was based on how the interaction happened: as an item regarding the data flow or a potential threat was brought up, it was recorded in the diagram and – in case of a threat or a clarification need – also into the notes. The next person to discuss usually continued building on what the previous contributor had said, indicating that they had combined and internalized the discussed knowledge into their own knowledge, before sharing this combined knowledge at their turn. The input from different participants was recorded in the data flow diagram as well as the notes.

6.2.2 Social capital

Social capital related enablers are considered as the most important enablers for knowledge creation (Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Bhatt 2000; Gold et al. 2001; Gupta & Govindarajan 2001; Fong 2003). Social capital consists of three dimensions: structural (consisting of organizational patterns of connections, their quality and structure, and the way they are implemented); relational (relationships that have been developing over time between individuals); and cognitive (shared resources) dimensions. (Nahapiet & Ghoshal 1998, 243-244). The impact of all three dimensions was observable in the cases analyzed for this study.

Structural capital

Structural capital contains network ties, network configuration and the appropriable organization (Nahapiet & Ghoshal 1998). In all three cases, structural capital had an observable impact on access to knowledge, and facilitator had an important role in supporting this. During the preparations, facilitators utilized their own perceptions of how the system would work in order to identify whether there would be any such interfaces that were significant for the analysis. Based on this, they discussed with the owner who then ensured that knowledge about these interfaces was available through workshop participants.

The impact of structural capital to knowledge access was most visible in case 2 where the facilitator had suggested including other teams to the workshop besides the initiating team. In a situation where external (third party) interfaces were in an important role, and the representation of that interface was not available, the solution was to acquire adequate information about the interface elsewhere – in case 1 from solution provider trainings, and in case 3 by self-studying before the workshop, as the facilitator had done.

Relational capital

Relational capital is situated within the network ties and personal relationships. It is formed through trust, norms, obligations and identification (Nahapiet & Ghoshal 1998). Rather clear demonstration of the impact of relational capital was observed in participant contribution; as already discussed in the previous section, the contributing participants engaged in knowledge creation based on the anticipated value and motivation, and their contribution became part of the common knowledge. The interviewees also mentioned other potential reasons for the participants not to contribute; based on their earlier experiences, group dynamics and existence/lack of culture (norms) of sharing failures could have a significant impact on contribution activity.

Another signal of the role of relational capital could be discovered in the connection between the initiating teams and the facilitators. In all cases, the owners described how they had decided to contact the facilitator, and they all expressed trust on the facilitators and their competences and ability to support them in reaching their objectives. The network ties (structural capital) between the owners and the facilitators as such enabled the possibility for making this contact but the relational capital seemed to be the driver for getting into contact. This follows the thinking of Adler & Kwon (2000, 100) when they describe structural capital and network ties as the context of creating knowledge, and relational and cognitive capital as the social capital embedded in the networks, impacting on how the networks operate.

Cognitive dimension

Nahapiet & Ghoshal (1998) see that the cognitive dimension of social capital has a significant impact on the capability to combine knowledge, and they mention shared

codes and language as well as shared narratives as the facets enabling this but also impacting access to knowledge and anticipation of value. As discussed in the previous section, the facilitators utilized a set of shared objects (such as data flow diagrams) and narratives (such as use cases), as well as shared language (STRIDE) during the workshop to build a common ground for knowledge exchange and combination. The workshop itself also acted as a shared context, including a shared objective, and offering channel for exchanging and combining knowledge.

From a wider perspective, the practice of conducting threat modeling workshops can be considered as a shared context enabling the combination capability, but also access to knowledge and anticipation of value. The workshops were all initiated by the teams, which means the teams knew that threat modeling workshops would be needed for creating adequate knowledge on the potential threats. The knowledge about threat modeling workshops and their benefits compared with other approaches (such as threat modeling done by the team or on an ongoing basis) in all three cases was originating from the earlier experiences of the initiating teams. This kind of shared collective experience supported selecting the facilitated workshops as the best way to reach the desired objectives, also facilitating the access to knowledge (of the facilitator and then the participants), and creating an anticipation of value (based on the earlier positive experiences).

6.2.3 Nature of knowledge

Chapter 2 of this study describes the nature of knowledge, especially its many characteristics and its dynamic and context-specific nature. When knowledge is converting through its different formats, also new knowledge is created. Knowledge creation involves continuous interaction between body of knowledge and knowing, and simultaneously between the four main dimensions of knowledge (Nonaka 1994; Blackler 1995; Spender 1996; Cook & Brown 1999; Nonaka et al. 2000).

Dynamic nature of knowledge

Knowledge is considered dynamic as it is constantly evolving; it is changing through the human interpretations and within social (including socio-technical) interaction. Knowledge at one moment within a certain context is not the same as at some other moment and in some other context. (Blackler 1995; Cook & Brown 1999; Nonaka

et al. 2000). In the workshops, the dynamic nature of knowledge was observable in many ways.

Starting with the preparations, any existing documentation about the systems in scope was not considered as a valid or up-to-date input for threat modeling workshop. It may have been that some of the participants would have relied in existing explicit documents when contributing in the discussions, but it was not possible to observe this, as the workshops were held online, and no such documentation was referred to during the workshops.

Instead of relying on existing materials, the knowledge exchange and combination took place during the workshops between the individuals contributing into the discussions, and it was based on their own experiences (experiential tacit knowledge) through their own work. In their contributions they shared their experiences and interpretations on collective tacit knowledge, such as organizational routines and ways of working that they had participated through their individual work roles. On the other hand, they also used the knowledge gained during the discussions and the shared experience of a threat modeling workshop to form new individual level knowledge. While it was relatively easy to follow the knowledge creation taking place around the data flow diagrams, this research did not focus on evaluating the individual level knowledge resulting from the workshop.

The workshop focused on creating collective knowledge on how the systems in the scope would work, what the potential threats would be, and what the participating teams should do next regarding these after the workshop. However, only a part of the knowledge created and shared during the workshop was captured into the data flow diagrams and notes, indicating that some of it was left in a tacit format. This was reflected in one of the interview comments stating that in case of not being able to finish the modeling in the set timeframe, it would not have been possible to continue later from where the workshop was left off.

Whereas the shared experience of participating the workshop can be seen as collective tacit knowledge, part of the tacit knowledge was potentially internalized by each of the participants through their own individual interpretation, and the documentation alone would not be enough to support recreating what was reached

in terms of shared understanding. This observation is in line with the dynamic and context-specific nature of knowledge (Nonaka 1994; Nonaka et al. 2000). The knowledge captured in the data flow diagrams was still considered useful: it was used as part of the notes to provide additional information on threats.

Observations on other characteristics of knowledge

Besides the four main categories of knowledge (explicit-tacit-individual-collective), Chapter 2 discusses five potential categorizations of knowledge that bring up aspects that are not included in the four main categories: 1) positive/negative knowledge (Teece 1998), 2) observable/non-observable knowledge (Teece 1998), 3) systemic/componential knowledge (Spender 1996), 4) autonomous/systematic knowledge (Teece 1998), and 5) embrained/embodied/encultured/embedded/ encoded knowledge (Blackler 1995). All these categories were identifiable in research material, impacting in different ways.

Chapter 2 mentions Teece's (1998) thoughts on whether the positivity/negativity of knowledge would impact the willingness to share that knowledge. Threat modeling is focused on identifying threats, which may be interpreted as negative knowledge. This aspect of knowledge was mainly brought up by the facilitators, as they were discussing the lack of culture of sharing failures as one the potential reasons limiting the contribution activity. They also mentioned that they aim at creating an open atmosphere which encourages bringing up the potential "problems" within the system. In the workshops, however, the participants who contributed were not afraid of sharing potential threats within their own responsibility areas.

Teece's (1998) categorization of knowledge being either observable or non-observable emphasizes the difference between assuming how something has been constructed and knowing how it has been constructed (having first-hand knowledge), and this was also identifiable in both the discussions and the interviews. In the preparations, one intention of workshop scoping was to avoid a situation where the knowledge about relevant interfaces and elements would not be available during the workshop. Also, when something was not observable (first-hand knowledge was not represented in the workshop), the participating team did not make any own assumptions but agreed to validate the knowledge with someone

who would know. This knowledge appeared to be most important in those situations where trust boundary crossing was discussed.

In case 1, those third-party solution related elements and interfaces that were not developed and run by the organization themselves, and thereby could be considered to contain “non-observable knowledge”, were considered to be “out-of-scope”. The teams trusted the solution provider to be available, in case any doubts about potential threats within these interfaces would have been raised during the workshop. However, the owner involved in case 1 also mentioned that the team is involved in security activities managed by the third-party solution provider regarding these interfaces, and also mentioned that the solution provider regularly reports the potential threats and shares regular security instructions with their partners. In this case, the knowledge that was non-observable from one angle (the organization) was still observable from another angle (solution provider), and the knowledge exchange and combination between the organization and its solution provider was considered to be on a level that provided the organization with adequate knowledge regarding potential threats.

The categorizations into systemic/componential knowledge (Spender 1996) and autonomous/systematic knowledge (Teece 1998) were also present in threat modeling workshops. One objective of workshop facilitation was to convert componential knowledge into systemic knowledge through the data flow diagram. This componential/systemic knowledge had a significant role throughout threat identification, as the componential knowledge supported understanding the potential weaknesses on the systemic level. The autonomous/systematic knowledge, or whether a certain change would have an impact in other parts of the system or not, was also discussed during the workshops on several occasions, and the discussions between the participants seemed to help clarify the impact of certain activities (e.g., in threat scenarios) to the rest of the system. In this sense, systemic/componential and autonomous/systematic characteristics of knowledge and especially recognizing these characteristics from threat modeling point of view had a fundamental role in the workshops.

The role of embodied and encultured knowledge

As discussed in Chapter 2, Blackler's (1995) five categories of knowledge contain aspects that overlap with the four main dimensions with two important distinctions: first, they consider encultured knowledge to align with shared understanding that is both an enabler of the knowledge creation process as well as its outcome, and second, they include an own category (embodied knowledge) for the tacit-explicit knowledge-related interaction between humans and material objects, such as technology.

Starting with the latter category, embodied knowledge was showing in the workshops as part of the individual contributions: as the participants described how the system works, they described both how it had been build (which can be considered as encoded knowledge) but also how they and the other human actors (such as potential threat actors) would interact with the system. As discussed in Chapter 2, this interaction also generates new knowledge (Blackler 1995), and the tacit knowledge/experience gained by the individual participants through this interaction and the comparison of individual experiences when discussing how the systems in scope would interact formed an important part of threat modeling.

The other distinctive category Blackler (1995) mentions is the encultured knowledge, which drives the ongoing process of social transformation. As discussed in Chapter 4, encultured knowledge can be considered as a source and output of shared context, and it is thereby an essential component in knowledge creation. (Blackler 1995). The whole analysis of threat modeling workshops from the viewpoint of knowledge creation provided an opportunity to view the role of social transformation in knowledge creation. As discussed in this chapter, it is visible from various angles: how knowledge is exchanged and combined, and simultaneously conversed through the SECI model; how the conditions of knowledge creation are formed; how the dimensions of social capital are present; how various forms and characteristics of knowledge impact; and naturally, how the whole shared understanding is formed within the process of knowledge creation.

Next and final chapter of this study, Chapter 7 continues the discussion on these findings in the context of knowledge management theories and concepts as well as concludes the key learnings from this study.

7 Conclusions

The main objective of this study is to understand knowledge creation in the context of threat modeling workshops, and how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context.

The research was conducted as qualitative case study, and the research material of this study consisted of three threat modeling workshops that were analyzed as separate cases as well as reflected to the theoretical based formed through various knowledge management theories and concepts introduced in Chapters 2, 3 and 4. An abductive reasoning logic was used throughout the research, enabling flexible probing between different theories, and resulting in an understanding of the significance of different theories and concepts related to the researched context.

Research motivation was in the end based on rather generic observations of the increasing amount of knowledge required for managing organization’s digital operations. Threat modeling workshops provided an opportunity to follow through knowledge exchange and combination targeted for creating knowledge for a specific purpose, and they proved to be an excellent research context for understanding, how the scattered knowledge about digital systems and operations can be brought together to create relevant new knowledge. Having the opportunity to follow through three different cases also increased the understanding on the impact of the context and scope of the workshops into knowledge creation.

This chapter discusses what can be concluded based on the analysis, what kind of managerial implications this would have, and what kind of an impact the research design and process had considering these outcomes.

7.1 Knowledge creation in threat modeling workshops

To understand how knowledge creation takes place in the context of threat modeling workshops, and how the nature of knowledge and different dimensions of social capital may impact knowledge creation in such context, altogether five research questions, one main question and four sub-questions, were formed:

A. What enables knowledge creation in cybersecurity threat modeling workshops? (main research question)
B. What is knowledge creation and how does it take place?
C. How do the different characteristics of knowledge impact knowledge creation?
D. How do the different aspects of social capital impact knowledge creation?
E. Which elements of knowledge creation can be identified in cybersecurity threat modeling workshops? (B-E as sub-questions)

The research started by describing the nature of knowledge and then proceeded to understand how it is created as well as what kind of role social capital has in knowledge creation. However, knowledge does have a dynamic nature, and the dynamic nature is both a reason for and a result of how knowledge creation takes place, and examining the nature of knowledge already provides an initial answer to the first of the sub-questions: **B. What is knowledge creation and how does it take place?**

Knowledge exists in various formats, and it has many different characteristics. When knowledge is converting through its different formats, also new knowledge is created. Individuals continuously interpret what they see and experience as well as interact both with other individuals and with their environment. Due to this interaction, individual knowledge continuously transcends and develops. Through interacting with others, an individual also contributes on how the knowledge of other individuals evolves. Experiencing social interaction also develops collective knowledge for the parties who have been involved. (Nonaka 1994; Cook & Brown 1999; Nonaka et al. 2000). Hence, knowledge creation is continuous conversion and transcendence of knowledge that takes place when individual interacts with their human and material surroundings.

SECI model describes the conversion of knowledge between its four main formats, and as knowledge is continuously evolving, also SECI takes place on both individual and collective levels and between explicit and tacit modes simultaneously and as a continuum (Cook & Brown 1999; Nonaka et al. 2000). Based on what knowledge creation is and how it takes place, another research sub-question can also be answered: **C. How do the different characteristics of knowledge impact knowledge creation?**

Different characteristics of knowledge impact knowledge creation in different ways. When knowledge is converting through its different formats, also new knowledge is created. Knowledge creation involves continuous interaction between body of knowledge and knowing, as well as between knowledge in different formats. The dynamic and context-specific nature of knowledge itself is the reason for as well as the result of knowledge creation. (Nonaka 1994; Cook & Brown 1999; Nonaka et al. 2000, Nonaka & Von Krogh 2009)

Altogether six different categorizations of knowledge were analyzed for this study. Four of these categories represent different interpretations of knowledge: is it considered negative or positive (Teece 1998), is it observable or non-observable (Teece 1998), is it systemic or componential (Spender 1996) or is it autonomous or systematic (Teece 1998). These interpretations depend on how knowledge is viewed and can be thereby seen rather as attitudes towards knowledge than descriptions of its essence. Recognizing these attitudes may help increasing the understanding of knowledge.

Two categorizations analyzed for this study are describing the essence and evolvement of knowledge: the four main categories of knowledge (explicit-tacit-individual-collective) discussed for example by Nonaka (1994), Spender (1996) and Cook & Brown (1999), and five categories of knowledge (embrained/embodied/encultured/embedded/encoded) evaluated by Blackler (1995). Regarding the four main categories of knowledge, the knowledge creation between the different formats is described with SECI model, explaining how the four main categories of knowledge impact knowledge creation (Cook & Brown 1999; Nonaka et al. 2000), whereas within the five categories of knowledge, the category of encultured knowledge

describes the social transformation of knowledge, and is seen as the key enabler for knowledge creation (Blackler 1995).

Knowledge is continuously created also without intentional facilitation, but knowledge can be also enabled with intentional activities. Most of these activities described in literature focus on different aspects of social interaction, and especially creating a shared context, and based on this, shared context seems to be an essential component on enabling knowledge creation in human interaction. (Blackler 1995; Nonaka et al. 2000) The importance of shared context in social interaction is based on its ability to enable exchanging and combining the tacit and explicit knowledge of individuals in a way that the individuals can at minimum make individual interpretations on each other's knowledge and – in some cases – also form shared understandings and new combinations based on each other's knowledge.

Even without mentioning the intentional facilitation, the researchers seem to agree that social systems and social capital has a significant role in knowledge creation. Sub-question D addresses this topic: **D. How do the different aspects of social capital impact knowledge creation?**

Among the manifold aspects of social capital in knowledge management literature, Nahapiet & Ghoshal's (1998) three dimensions of social capital (structural, relational, and cognitive) and their impact on four conditions of knowledge exchange and combination were analyzed and it was concluded that while social capital can impact the conditions needed for creating knowledge, there are also many connections among the three dimensions of social capital and many indirect and direct impacts between the dimensions and the conditions.

Whereas all the four conditions of access to knowledge, anticipation of value, motivation, and combination capability need to be in place to enable knowledge creation (Nahapiet & Ghoshal 1998), it also seems – among these conditions – the definition of combination capability in Nahapiet & Ghoshal's original work is rather narrow. They include two facets into combination capability, representing shared language and codes, and shared narratives, while the concept of shared context also includes other aspects, such as knowledge overlap (redundancy), knowledge

assets (underlying knowledge in its different formats), and “ba”, a shared time and place context. (Grant 1996; Nonaka et al. 2000; Fong 2003).

The results of this research indicate that both the four conditions (Nahapiet & Ghoshal 1998) and the shared context (Blackler 1995; Grant 1996; Nonaka et al. 2000) are essential for knowledge creation. Whereas Nahapiet & Ghoshal present certain causal relations between the three dimensions of social capital and the four conditions of knowledge exchange and combination, also similar relations can be observed between social capital and shared context and those elements of shared context that were discussed in this study.

Based on the reviewed literature, neither the relations described by Nahapiet & Ghoshal or the relations identified between social capital and shared context can be considered straightforward and free of various mutual interdependencies. It can be concluded that social capital impacts knowledge creation, as it can promote or hinder the four conditions as well as the creation of shared context. However, a deeper analysis of this impact would be required to properly understand and describe it.

Among the elements of knowledge creation analyzed for this study, especially the social capital related aspects and the different characteristics of knowledge as well as the potential mechanisms used for supporting knowledge creation were monitored during the empirical research to be able to respond to sub-question **E. Which elements of knowledge creation can be identified in cybersecurity threat modeling workshops?**

As the empirical analysis was done simultaneously with the theoretical research, the approach had an impact on both the interpretations of the theory and the understanding formed through the empirical material. From the viewpoint of this research question this means that the elements of knowledge creation highlighted in the theoretical research were also those ones that were identifiable in the empirical context, the threat modeling workshops. Instead of this sub-question, it would therefore be more important to discuss the main research question **A. What enables knowledge creation in cybersecurity threat modeling workshops?** as answering this question also enables answering to the sub-question E.

Threat modeling workshops offered an excellent opportunity to monitor intentional knowledge creation that took place in a pre-planned context that was set up particularly to enable knowledge exchange and combination. It was potentially due to the pre-organized nature of the workshops that the four conditions of knowledge exchange and combination (Nahapiet & Ghoshal 1998), were rather observable in both preparations of the workshop as well as during the workshop. The preparations focused on ensuring the access to knowledge, anticipation of value and motivation. The two latter, however, were also enabled without intentional activities, mainly based on the expectations set by the organization. The facilitators continued ensuring these conditions also during the workshop, while they were also focusing on enabling the combination capability by promoting the use of shared language, codes, and narratives. (Nahapiet & Ghoshal 1998).

Each threat modeling workshop itself also had all the qualities of a shared context, as it was based on shared purpose and objectives and it was also connecting the participants to each other via time and space, similarly to what has been described as part of the concept of “ba” (Nonaka et al. 2000). Threat modeling as an activity utilized shared objects and language to facilitate knowledge exchange and combination between the participants (Nahapiet & Ghoshal 1998; Nonaka et al. 2000; Fong 2003). The participants contributed by bringing in their individual contexts and knowledge (Nahapiet & Ghoshal 1998, Nonaka et al. 2000), and the overlap of knowledge between different parties, including the facilitator, supported their interaction (Grant 1996; Nonaka et al. 2000).

Facilitation and especially questions used for steering the work were both targeting at activating the participants to get their contribution as well as creating a shared understanding and supporting the interpretations made based on the discussion. (Nahapiet & Ghoshal 1998). Shared objects, language and facilitation also supported the continuous knowledge conversion between its four main modes (Nonaka et al. 2000). Even though the actual SECI model (Nonaka 1994; Nonaka et al. 2000) of knowledge conversion was not specifically at the focus of this research, it was observable through the explicit knowledge objects (data flow diagram, notes, discussions) and how these were developing during the workshop.

The interaction within each workshop was enabled by social capital: the structural dimension of social capital supported the access to knowledge, while relational and cognitive dimensions were more visible in the interaction between the participants as well as between the participants and the facilitator (Nahapiet & Ghoshal 1998). The workshops were structured to enable effective exchange and combination of knowledge: first, a shared understanding of the scope was formed, and this was followed by threat identification which was the actual objective of the work. In this sense, the dynamic and context-specific nature of knowledge were both considered: the threat modeling workshop as a context did require specific knowledge formed to serve the particular purpose and the shared understanding needed to be formed to capture the knowledge for this purpose. (Blackler 1995; Nonaka et al. 2000)

Regarding different characteristics of knowledge, the four categorizations based on how knowledge can be interpreted (Spender 1996; Teece 1998) were considered throughout threat modeling workshops, and these “attitudes” were continuously probed and reformed with the help of facilitation. Whereas the knowledge of threats and risks was categorized as “negative” by Teece (1998), the attitude towards this kind of information during the workshops was positive even without facilitation, as the participants knew the intention of the workshops was to specifically focus on this type of knowledge. The observability of knowledge as well as its seemingly autonomic and componential characteristics were both continuously evaluated by the facilitator and the participants during the discussions, and viewed from different angles to identify whether something was relevant or not regarding the workshop objectives (Spender 1996; Teece 1998).

The dynamic and context-specific nature of knowledge (Nonaka 1994; Blacker 1995; Cook & Brown 1999; Nonaka et al. 2000) was at the core of the whole idea of arranging threat modeling workshops in the first place, and it was crystallised in one expression repeating in the interviews of the facilitators: *You should not assume someone doing something*. As the knowledge related to digital systems also continuously evolves, all the documented knowledge and the discussions one may once had with their colleagues may not reflect the current situation.

Due to the dynamic and context-specific nature of knowledge, it would not be possible to fully describe how these elements and the actual knowledge creation

took place during the cybersecurity threat modeling workshop. The following Figure 20 describes how the elements of knowledge creation were observed during the workshops. Different layers of the circle describe the elements that were the most recognizable during the workshops: the core is built around the knowledge conversion/creation (described by SECI in the figure for clarity). Shared context (the second inner layer) is the ultimate prerequisite for knowledge creation, whereas the four conditions of knowledge creation (third inner layer) need to be in place in order to enable the shared context, knowledge exchange and combination. Three dimensions of social capital impact the inner layers but also each other. Finally, the nature of knowledge, especially its dynamic and context-specific nature, impacts all the layers of the circle.

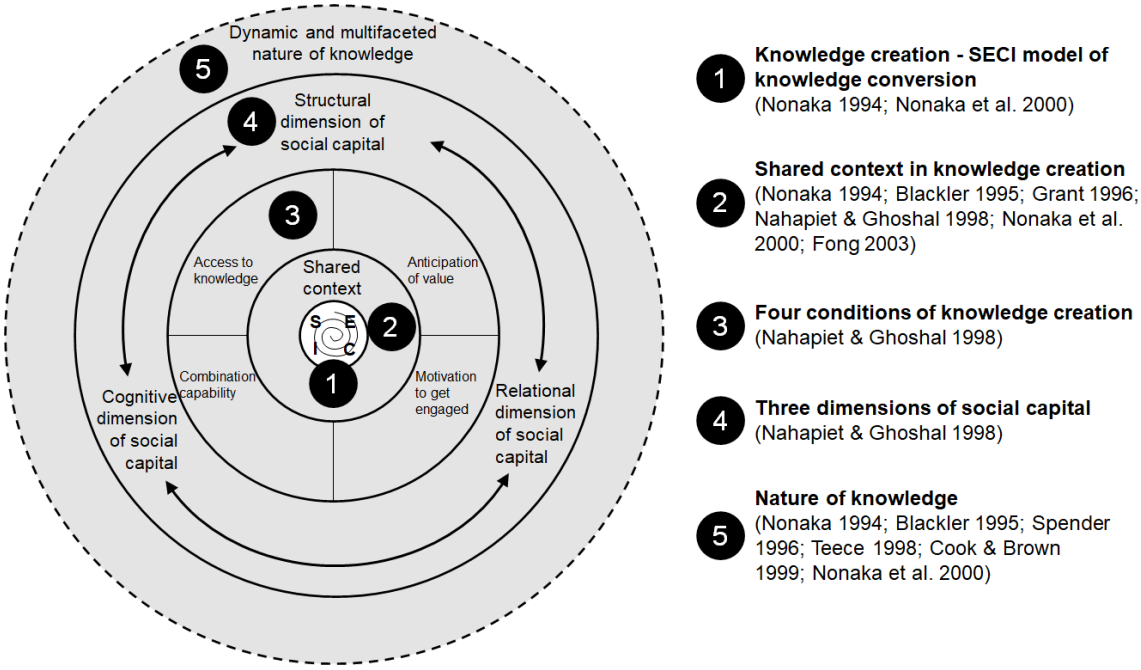


Figure 20. Knowledge creation in threat modeling workshops.

Knowledge creation takes place in cybersecurity threat modeling workshops through social interaction between the participants and within the shared context (Spender 1996, 47; Cook & Brown 1999; Nonaka et al. 2000).

Knowledge creation does not take place unless its conditions are met: access to knowledge, anticipation of value, motivation to get engaged and the combination capability, as well as the shared context should be in place for knowledge exchange

and combination to take place. (Nonaka 1994; Blackler 1995; Grant 1996; Nahapiet & Ghoshal 1998; Nonaka et al. 2000)

The three dimensions of social capital feed each other and enable the conditions for knowledge exchange and combination both directly and indirectly. (Nahapiet & Ghoshal 1998).

Nature of knowledge impacts in two ways: 1) different attitudes towards knowledge (Spencer 1996; Teece 1998) need to be understood and challenged to improve the knowledge creation potential, and 2) knowledge, being dynamic and context-specific, needs to be understood that it is constantly evolving, and any assumptions done without proper validation may result in situations where the quality of threat modeling is not where it could be. (Nonaka 1994; Cook & Brown 1999; Nonaka et al. 2000)

7.2 Managerial implications

In the research objectives, it was mentioned that – depending on the relevancy of the research findings – this study may also provide some practical ideas for developing threat modeling workshops. Instead of practical ideas to be directly applied to threat modeling workshops, the study resulted in some key observations that may be useful for organizations practicing threat modeling. These observations are linked to empirical research rather than theoretical analysis and can thereby be considered to have a more practical nature even though they do not contain any practical instructions or guidelines.

Threat modeling is a continuous activity. Throughout the empirical research, the discussions included a lot of remarks on threat modeling as an activity that should be done in all possible situations: when considering different alternatives in the design phase, when building something that requires new features, before something is implemented, or after it is already in use, just to name a few aspects. Threat modeling can be done on a micro-level (one person considering one element) but also on a larger scale. Based on the interviews it does not necessarily require using an arsenal of tools and methods – it can be simply done by considering what could go wrong if something is done. However, in all levels of threat modeling,

it seems to be crucial to understand what exactly is analyzed to identify potential threats. This leads to another key observation.

Viewpoint matters a lot. It was obvious in all cases that scoping is a key activity when planning threat modeling; it impacts on what is required for the actual threat modeling workshop in terms of available knowledge, time, and effort. Those parts of the scope that were potentially non-observable from one participant's viewpoint were fully observable for others, and whereas a certain change might have seemed to be an autonomous one, in many situations it was concluded to have an impact also on other parts of the system. It seems to be extremely important to gain a good level of understanding of the scope and potential areas of impact related to those activities that trigger the threat modeling need in the first place before deciding on how the threat modeling should be done and who should be involved. Based on this, yet another key observation seems relevant.

DIY vs someone else as a facilitator. Even though this decision was described by the owners in each of the cases, it would be difficult to make any strong conclusions on when it would be best to involve an external facilitator into threat modeling. The facilitators described their role almost purely as a facilitating one, steering the discussion with open questions and ensuring the scope would be covered, whereas the owners also considered the facilitators to possess valuable understanding of the context. Regarding the content of the workshops, facilitator's knowledge was the most useful when there was a need to identify connections and causal relations between elements. In all cases, the facilitator had a significant role also in supporting the definition of the scope and identifying the knowledge needed for the analysis: They were for example evaluating what could be covered during the planned timeframe (based on how they evaluated the complexity of the scope) or whether the planned participants did have adequate knowledge to cover all the relevant interfaces on the planned scope. They also had an important role in keeping the discussion within threat identification instead of discussing the solutions, and thereby ensuring the whole scope was covered before moving into planning the actions. The actions resulting from the workshop led to the fourth and probably the most practical observation.

Keeping track on the status. In all three cases, the teams involved in threat modeling had work management systems and they were using backlogs to manage their tasks. This seemed extremely important from the effectiveness viewpoint: as all the identified issues were converted to work tickets, all of them were viewed at least to decide, what kind of priority each of the tasks would have in the backlog, and who would have the main responsibility of each task. In case 1, the team mentioned several times that they already had some activities ongoing that would simultaneously help mitigating the threats identified in the workshop, and – due to their work management practices – they were also able to link the identified threat into the already ongoing work in their system.

In addition to these four observations, numerous other remarks were made during the research. These also included some observations on the limitations of the research.

7.3 Limitations and suggestions for further research

During this study it became obvious that knowledge creation, its enablers, as well as knowledge itself, have been widely studied. Previous research has produced various theories and concepts, which are mostly interlinked and overlapping. Approaching the research target purely by using the empirical data to test the theories and concepts examined in the literature review (deductive analysis approach) or to trying to form an understanding of potential theories and concepts that could be identified based on three individual cases (inductive analysis approach) both seemed to increase the likelihood of making relatively straightforward conclusions.

Examining the complex and dynamic nature of knowledge and the process of knowledge creation did however require a review of what had been studied and proposed previously regarding the topic. Theoretical review (forming the Chapters 2, 3 and 4 of this study) was crucial for establishing a research position, designing the empirical research approach, and making sense of the research findings. During the process of analyzing the theoretical and empirical material simultaneously, some of the theories and concepts seemed more relevant than others. The abductive reasoning approach supported finding the most relevant theories and concepts to describe the knowledge creation in the selected context.

Besides selecting a suitable reasoning logic for this research, also setting a suitable research objective proved to be somewhat challenging. Originally, the main research question was worded as “How does knowledge creation take place within threat modeling workshops”, and it was loaded with additional aspects that also needed to be covered: “How the nature of knowledge capital may impact knowledge creation in such context” and “How the different dimensions of social capital may impact knowledge creation in such context”.

When the empirical data was gathered, the original main research question “How knowledge creation takes place within threat modeling workshops?” was still considered valid. However, during the several iterations of data analysis, it started to look like that understanding how knowledge creation took place within the workshops would have required a more solid empirical research, focusing on content and development of the knowledge itself, for example by comparing the individual and collective knowledge before and after the workshop, or describing the detailed process of (explicit) knowledge creation in each of the workshops. Instead, the data gathering approach that had been used (semi-structured interviews and workshop observations) seemed to produce insight on what kind of elements had been supporting/enabling the knowledge creation during threat modeling workshops. Based on this observation, the main research question was changed during the study to better describe the research findings: “What enables knowledge creation in cybersecurity threat modeling workshops?”.

The research material consisted of three cases, which represented three threat modeling workshops. An adequate amount of research material was gathered during the research – altogether 310 minutes of workshop recordings as well as 574 minutes of interview recordings, accompanied with the workshop presentations, documentations and screenshots – yet, the material only enabled scratching the surface on what might enable knowledge creation in threat modeling workshops.

Besides its primary objective to understand knowledge creation in the context of threat modeling workshops, the secondary objective of this study was to increase the researcher’s own understanding on knowledge creation and knowledge management theories. This research also served this purpose but on the side, it also provided a lot of insight on how the knowledge management research field has

been structured and how this could have been considered when designing the research scope and objectives as well as the selected approach and methodology. To gain even deeper insight on knowledge creation in threat modeling workshop, there seems to be a lot of room for further research on the same context:

1) Focusing on one core theory and the related concepts and testing the (non-organized) existing research material using a deductive approach
2) Expanding the research material with additional cases using the same data gathering approach to test the findings from this research
3) Expanding the research material with additional data gathering methods such as surveys or longer follow-up period (for example following through the tasks generated as a result of the threat modeling workshops)
4) Including also other knowledge management related theories and concepts than the basic knowledge management theories selected for the study, especially those developed in the field of computer science to utilize findings from other similar contexts.

Despite the various limitations and challenges discussed above, the research approach proved to be fruitful from the researcher's perspective, and it provided valuable input from the perspectives of both the primary and the secondary objectives. As research contexts, both cybersecurity related knowledge as well as understanding knowledge management enablers and challenges related to the growing amount of socio-technological knowledge within organizations are more than likely to remain relevant also in the future.

Literature

Adler & Kwon (2000). Social capital: The good, the bad and the ugly. In Lesser, E.L. (2000). Knowledge and social capital: Resources for knowledge-based economy. Butterworth-Heinemann.

Alavi, M. & Leidner, D. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS Quarterly, 25, 1, 107-136.

Ayres, L. (2012). Semi-structured interview. Published in Given, L.M. (Ed.). The SAGE Encyclopedia of Qualitative Research Methods, 811.

Babar, M. A. & Gorton, I. (2007). Architecture Knowledge Management: Challenges, Approaches, and Tools. 29th International Conference on Software Engineering, IEEE Computer Society.

Bamberger, P.A. (2018). AMD - Clarifying what we are about and where we are going. Academy of Management Discoveries 2018, Vol. 4, No. 1, 1–10.

Berger, R. (2013). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. Qualitative Research, Vol. 15, No. 2, 1-16.

Bhatt, G.D. (2001). Knowledge management in organizations: examining the interaction between technologies, techniques, and people. Journal of Knowledge Management, Vol. 5, No. 1, 68-75.

Blackler, F. (1995). Knowledge, knowledge work and organizations: An overview and interpretation. Organization studies, Vol. 16, No. 6, 1021-1046.

Blatter, J.K. (2012). Case studies. Published in Given, L.M. (Ed.). The SAGE Encyclopedia of Qualitative Research Methods, 68-71.

Capilla, R., Jansen, A., Tang, A., Avgeriou, P. & Babar, M.A. (2016). 10 years of software architecture knowledge management: Practice and future. The Journal of Systems and Software, Vol. 116, 191–205.

Cook, S.D.N. and Brown, J.S. (1999). Bridging Epistemologies: The generative dance between organizational knowledge and organizational knowing, Organization Science Vol. 10, No. 4, 381–400.

Davenport, T., and Prusak L. (1998). Working Knowledge, Harvard Business School Press, Boston.

Dubois, A. & Gadde, L-E. (2002). Systematic combining: an abductive approach to case research. Journal of Business Research, Vol. 55, 553–560.

Dunning, D. (2011). Chapter five - The Dunning–Kruger Effect: On Being Ignorant of One's Own Ignorance. Advances in Experimental Social Psychology. Vol. 44, 247-296.

Earl M. (2001). Knowledge management strategies: Toward a taxonomy. Journal of Management Information Systems, Vol. 18, No. 1, 215-233.

ENISA, European Union Agency for Cybersecurity (2019). Inventory of Risk Management/Risk Assessment Methods. Available online at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods . Accessed December 29, 2019.

Ferenhof, H.A., Durst, S., Bialecki, M.Z., & Selig, P.M. (2015). Intellectual capital dimensions: state of the art in 2014. Journal of Intellectual Capital Vol. 16 No. 1, 58-100.

Fong, P.S.V. (2003). Knowledge creation in multidisciplinary project teams: An empirical study of the processes and their dynamic interrelationships. International Journal of Project Management, Vol. 21, 479-486.

Gartner (2017). Build adaptive security architecture into your organization. Available online at https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/ Accessed January 3, 2020.

Given, L.M. & Saumure, K. (2012). Trustworthiness. Published in Given, L.M. (Ed.). The SAGE Encyclopedia of Qualitative Research Methods, 896.

Gold, A.H., Malhotra, A. & Segars, A.H. (2001). Knowledge Management: An Organizational Capabilities Perspective. Journal of Management Information Systems, Vol. 18, No. l, 185-214.

Grant, R. (1996). Toward a knowledge-based theory of the firm. Strategic Management Journal, Vol. 17, 109-122.

Grundstein, M. (2013). Towards a technological, organizational, and socio-technical well-balanced KM initiative strategy: a pragmatic approach to knowledge management. Knowledge Management Research & Practice, Vol. 11, 41–52.

Gupta, A.K. & Govindarajan, V. (2000). Knowledge Management's Social Dimension: Lessons From Nucor Steel MIT Sloan Management Review, 42, 1, 71-80.

Handzic, M. (2017). The KM Times They Are A-Changin´. Journal of Entrepreneurship, Management and Innovation (JEMI), Vol 13, Issue 3. 7-27.

Heisig, P. (2009). Harmonisation of knowledge management – comparing 160 KM frameworks around the globe. Journal of Knowledge Management, 13, 4. 4-31.

Hirsjärvi S., Remes, P. & Sajavaara P. (2007). Tutki ja kirjoita. Otavan Kirjapaino Oy, 13. osin uudistettu painos.

Hussinki, H., Kianto, A., Vanhala, M. & Ritala, P. (2017). Assessing the universality of knowledge management practices. Journal of Knowledge Management, Vol. 21, No. 6, 1596-1621.

Kalogeraki, E-M., Apostolou, D., Polemi, N. & Spyridon, P. (2018). Knowledge management methodology for identifying threats in maritime/logistics supply chains. Knowledge Management Research & Practice, Vol. 16, No. 4, 508-524).

Kianto, A. & Waajakoski, J. (2010). Linking social capital to organizational growth. Knowledge Management Research & Practice, Vol. 8, 4–14.

Kogut, B. & Zander, U. (1992). Knowledge of the firm, combinative capabilities, and the replication of technology. Organization Science, 3, 3, 383-397.

Käpylä, J., Kujansivu, P. & Lönnqvist, A. (2012). National intellectual capital performance: a strategic approach. Journal of Intellectual Capital Vol. 13 No. 3, 343-362.

Lam A. (2000). Tacit knowledge, organizational learning and societal institutions: An integrated framework. Organization studies 21/3. 485-531.

Leonardi, P.M. & Barley S.R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. Information and Organization, Vol. 18, 159-176.

Lesser, E.L. (2000). Leveraging social capital in organizations. In Lesser, E.L. (2000). Knowledge and social capital: Resources for knowledge-based economy. Butterworth-Heinemann.

Mantere, S. & Ketokivi, M. (2013). Reasoning in organization science. Academy o/ Management Review, Vol. 38, No. 1, 70-89.

Marr, B. (2008). Impacting future value: How to manage your intellectual capital. The Society of Management Accountants of Canada (CMA Canada), the American Institute of Certified Public Accountants, Inc. (AICPA) and The Chartered Institute of Management Accountants (CIMA), 1-34.

McElroy, M.W. (2002). Social innovation capital. Journal of Intellectual Capital,Vol. 3 No. 1, 30-39.

McKechnie, L. F. M. (2008). Observational research. Published in Given, L.M. (Ed.). The SAGE Encyclopedia of Qualitative Research Methods, 574-576.

Nahapiet, J. & Ghoshal, S. (1998). Social capital, intellectual capital and the organizational advantage. Academy of Management Review, Vol. 23. No. 2, 242-266.

NIST, National Institute of Standards and Technology (2018). Framework for improving critical infrastructure cybersecurity. Available online at https://doi.org/10.6028/NIST.CSWP.04162018. Accessed December 28, 2019.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation, Organization Science, Vol. 5, No. 1, 14-37.

Nonaka, I. (2007). The knowledge creating company, republication of the 1991 article. Harvard Business Review, July - August. Available online at https://hbr.org/2007/07/the-knowledge-creating-company . Accessed January 26, 2020.

Nonaka, I & Takeuchi, H. (1995). The knowledge-creating company. Oxford University Press, New York.

Nonaka, I., Toyama, R. & Konno, N. (2000). SECI, Ba and Leadership: a unified model of dynamic knowledge creation. Long Range Planning, 33, 5-34.

Nonaka, I. & Von Krogh, G. (2009). Tacit Knowledge and Knowledge Conversion: Controversy and Advancement in Organizational Knowledge Creation Theory. Organization Science, Vol. 20, No. 3, 635–652.

Orlikowski, W. J. (2007). Sociomaterial Practices: Exploring Technology at Work. Organization Studies, Vol.28 (9), 1435-1448

Padgett, D.K. (2017). Qualitative methods in social work research. SAGE Publications, Inc.

Parviainen, J. & Eriksson, M. (2006). Negative knowledge, expertise and organisations. International Journal of Management Concepts and Philosophy, Vol. 2, No. 2, 140-153.

Patton, M.Q. (2012). Evaluation Criteria. Published in Given, L.M. (Ed.). The SAGE Encyclopedia of Qualitative Research Methods, 302-303.

Pinho, I., Rego, A. & Pina, M. (2012). Improving knowledge management processes: a hybrid positive approach. Journal of Knowledge Management,Vol. 16, No. 2, 245.252.

Polanyi, M. (1958). Personal knowledge: Towards a post-critical philosophy. Routledge & Kegan Paul Ltd, 1962 corrected edition.

Robey, D., Anderson, C. & Raymond, B. (2013). Information Technology, Materiality, and Organizational Change: A Professional Odyssey. Journal of the Association for Information Systems Vol. 14, No. 7, 379-398.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information Science, Vol. 33, No. 2, 163–180.

Sallos, M.P., Garcia-Perez, A., Bedford, D. & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital,Vol. 20, No. 4, 581-597.

Salonius, H. & Lönnqvist, A. (2012). Exploring the policy relevance of national intellectual capital information. Journal of Intellectual Capital Vol. 13 No. 3, 331-342.

Schoenfield, B.S.E. (2015). Securing systems: Applied security architecture and threat models. CRC Press, Taylor & Francis Group.

Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons, Inc.

Serenko, A. & Bontis, N. (2016). Understanding counterproductive knowledge behavior: antecedents and consequences of intra-organizational knowledge hiding. Journal of Knowledge Management, Vol. 20, No. 6, 1199-1224.

Souag, A., Mazo, R., Salinesi, C. & Comyn-Wattian, I. (2016). Reusable knowledge in security requirements engineering: a systematic mapping study. Requirements Engineering, Vol. 21, 251–283.

Spender, J.C. (1996). Making knowledge the basis of a dynamic theory of the firm. Strategic Management Journal, Vol. 17, 45-62.

Staller, K.M. (2012). Epistemological boot camp: The politics of science and what every qualitative researcher needs to know to survive in the academy. Qualitative Social Work, Vol. 12 (4), 395–413.

Takeuchi, H. & Nonaka, I. Classic work: Theory of organizational knowledge creation. In Morey, D., Maybury, M. T., Thuraisingham, B.M. (2002). Knowledge Management: Classic and contemporary works. MIT Press. 139-182.

Teece, D.J. (1998). Capturing value from knowledge assets: The new economy, markets for know-how, and intangible assets. California Management Review (44:3). 55-79.

Timmermans, S. & Tavory, I. (2012). Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis. Sociological Theory, Vol. 30(3), 167 –186.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective. Issues in Information Systems, Vol. 16, Issue III, 191-198.

Tuomi, J. & Sarajärvi, A. (2009). Laadullinen tutkimus ja sisällönanalyysi. Tammi, 6. uudistettu laitos.

Visconti, L.M. (2010). Ethonographic case study (ECS): Abductive modeling of ethnography and improving the relevance in business marketing research. Industrial Marketing Management, Vol. 39, 25-39.

Yin, R.K. (2017). Case study research and applications: Design and methods. Sage Publications.

Zimmermann, O., Miksovic, C. & Küster, J.M. (2012). Reference architecture, metamodel, and modeling principles for architectural knowledge management in information technology services. The Journal of Systems and Software, Vol. 85, 2014-2033.

Appendix 1. Pre-workshop interview structure

Interview themes	Interview questions	Link to research questions	Theories and concepts
Background and objectives	• Please describe this upcoming threat modeling workshop. What is it about? Why is it held? • What are the objectives for this workshop?	• What is knowledge creation and how does it take place?	• Nature of knowledge
Workshop setup	• Where will the workshop be held? • How did you select the participants for this session? • Who will participate the session? Why?	• What is knowledge creation and how does it take place?	• Knowledge creation and different enablers and elements • Social capital: cognitive, structural and relational dimensions
Preparations	• What kind of preparations have been made for this session? • Who has participated in the preparations and how? • How have you participated the preparations?	• How do the different characteristics of knowledge impact knowledge creation? • How do the different aspects of social capital impact knowledge creation?	• Nature of knowledge • Social capital: cognitive, structural and relational dimensions
Agenda and process	• How have you planned this session to be conducted? (agenda, participation, methods) • What will be your role during the session (and what would this mean/include)? • What do you expect from the facilitator/owner during the session?* • What do you expect from the participants during the session?	• What is knowledge creation and how does it take place? • How do the different aspects of social capital impact knowledge creation?	• Knowledge creation and different enablers and elements • Social capital: cognitive, structural and relational dimensions
Deliverables and outcomes	• What kind of outcomes are expected from the session? • What needs to happen in the session to reach the set objectives? • What could hinder the team from reaching these objectives? • What are your personal expectations for the session? • What from your point of view should happen after the session?	• What is knowledge creation and how does it take place? • How do the different characteristics of knowledge impact knowledge creation?	• Knowledge creation and different enablers and elements • Nature of knowledge • Social capital: cognitive, structural and relational dimensions
Other	• What else you would like to share?		

* Question about the facilitator addressed to the owner and vice versa.

Appendix 2. Post-workshop interview structure

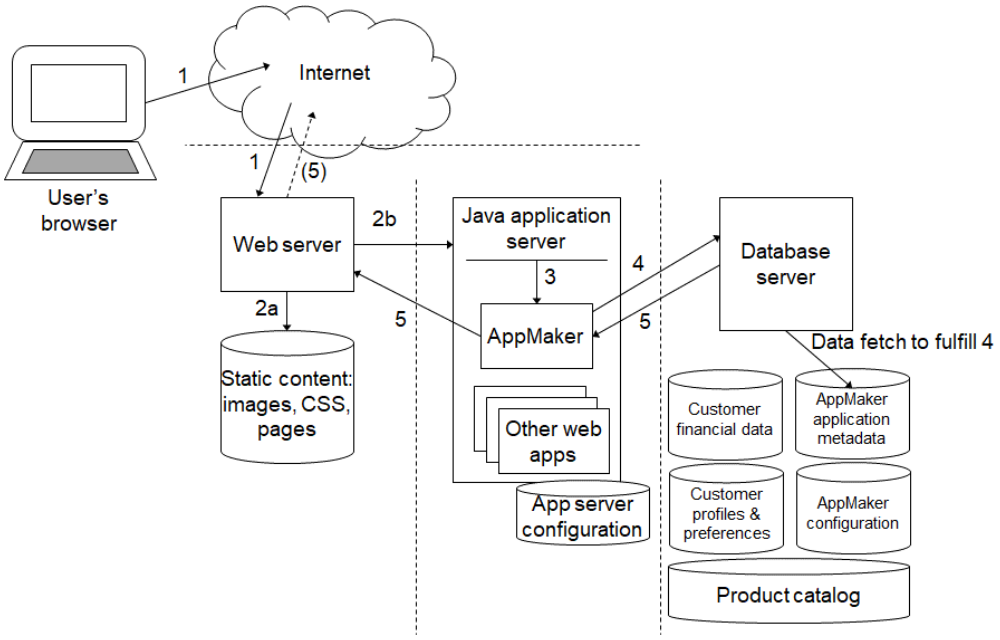
Interview themes	Interview questions	Link to research questions	Theories and concepts
First impressions	• How did you find the session to meet your expectations? • What went well? • What did not go that well?	• What is knowledge creation and how does it take place?	• Knowledge creation and different enablers and elements
Agenda and process	• How was the session conducted? • What kind of role did the facilitator have? • What kind of role did the owner have?	• What is knowledge creation and how does it take place? • How do the different aspects of social capital impact knowledge creation?	• Knowledge creation and different enablers and elements • Social capital: cognitive, structural and relational dimensions
Workshop setup (place, participants)	• How was the participation of this session? • What kind of roles did the participants have in the session? • What kind of input did the participants bring into the session? • How did the contribution meet your expectations? • What would you have changed regarding participation? Was anybody missing?	• What is knowledge creation and how does it take place? • How do the different characteristics of knowledge impact knowledge creation? • How do the different aspects of social capital impact knowledge creation?	• Knowledge creation and different enablers and elements • Nature of knowledge • Social capital: cognitive, structural and relational dimensions
Deliverables and outcomes	• What were the most important outcomes the session? (implicit, explicit) • How do the outcomes meet the objectives? Is anything missing? Is there anything surprising did not expect? • What would you say were the key takeaways from the session? • How were your personal expectations met during the session? Why? • What did not go as expected? Why? • What did you personally learn during the session? • What could have been done differently? • What will now happen next after the session?	• What is knowledge creation and how does it take place? • How do the different characteristics of knowledge impact knowledge creation? • How do the different aspects of social capital impact knowledge creation?	• Knowledge creation and different enablers and elements • Nature of knowledge • Social capital: cognitive, structural and relational dimensions
Other	• What else would you like to share?		

Appendix 3. Data flow diagrams (Schoenfield 2015)

In their book “Securing systems: Applied security architecture and threat models”, Brook S. E. Schoenfield calls data flow diagrams created as part of threat modeling as tools for “decomposing architecture to a functional granularity such that these units can be factored into security significant components”. They explain that, as there are so many different views of the architecture and each of these views may include information that would be relevant for threat identification (or security activities in general), this information should be combined in order to analyze it. (Schoenfeld, 2015, 98).

Data flow diagrams drawn for threat modeling purposes can consist of but are not limited to (Schoenfield 2015): 1) Components/elements/systems or any logical architecture (servers, repositories, applications, software, browsers, etc.); 2) Communication flows to exchange data or control messages, including their directions (usually as arrows); 3) Trust boundaries; 4) Data types; 5) Information on the order of the flow (e.g. arrows numbered in chronological order); and 5) Security controls/components.

In the below example of a data flow diagram, all except security controls are presented.



Example of a data flow diagram (Schoenfield 2015, 155).

Appendix 4. STRIDE model for threat identification (Shostack, 2014)

STRIDE, originally developed by Kohnfelder and Garg, is formed through the first letters of six threat types: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. In their book “Threat modeling: Designing for security”, Adam Shostack names STRIDE as “framework and mnemonic”, emphasizing it is intended as a guidance, and not as a point-to-point checklist for threat identification. (Shostack 2014, 61).

The following table (based on Shostack 2014, 62-63) describes the general level threat types included in STRIDE.

Threat	Property violated	Threat definition	Typical victims
Spoofing	Authentication	Pretending to be something or someone other than yourself	Processes, external entities, people
Tampering	Integrity	Modifying something on disk, on a network or in memory	Data stores, data flows, processes
Repudiation	Non-repudiation	Claiming that you did not do something, or were not responsible. Repudiation can be honest or false, and the key question for system designers is what evidence they have	Process
Information disclosure	Confidentiality	Providing information to someone not authorized to see it	Processes, data stores, data flows
Denial of service	Availability	Absorbing resources needed to provide service	Processes, data stores, data flows
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do	Process

Appendix 5. Documents created as part of the workshops

(based on the interviews and workshop observations).

Document	Initiation	Preparations	Workshop	Follow-up
Work ticket for threat modeling workshop	Team or person initiating threat modeling creates a ticket describing the need and scope of the threat modeling into the work management system	Owner (and their team) and facilitator discuss the scope Owner updates the ticket	DFD and workshop minutes and notes are added in the threat modeling work ticket and shared with all participants	Work ticket for threat modeling workshop can be considered done (and the work approved) when it includes the workshop documentation and work tickets have been created in the backlogs based on all the findings
Data flow diagram (DFD) describing the scope and findings			DFD is created in co-operation between the participants during the workshop Findings are included in, or at least linked with the data flow diagram during the discussion	DFD becomes part of the work ticket of the threat modeling in question
Workshop minutes and notes			Workshop participants, minutes, threat modeling findings and other actions are recorded in the notes in a format that enables to convert them into work tickets after the workshop	Workshop minutes and notes are used for creating new work tickets Workshop minutes and notes become part of the work ticket of the threat modeling in question
Work tickets from threat modeling				Work tickets are created based on workshop minutes and notes, and linked to the original work ticket for threat modeling workshop Work tickets are prioritized and monitored by the related backlog owner(s)