Facilitating Cyber Security Threat Modelling: A Social Capital Perspective

Johanna Orjatsalo
LUT University, School of Business and Management, Lahti, Finland
johanna.orjatsalo@lut.fi

Abstract: To identify and manage their cyber security risks, organisations need to form a thorough understanding of various factors that may expose them to these risks. While cyber security professionals and scholars have developed a plethora of practical methodologies and frameworks to support cyber security risk identification and mitigation, the theoretical foundations on what promotes effective knowledge creation when using these methodologies and frameworks are nascent. Yet, theories developed in the field of knowledge management and intellectual capital may provide valuable insight on how to enhance cyber security risk related knowledge creation in organisations. For example, social capital is considered as an important prerequisite for knowledge exchange and combination when creating new intellectual capital (Nahapiet & Ghoshal, 1998). However, more focused research is required to understand how social capital affects knowledge creation in the context of organisational cyber security risk related activities. Using qualitative data gathered from three cyber security threat modelling workshops, this paper examines how social capital enables conditions for exchanging and combining knowledge on cyber security threats. By comparing the empirical observations with Nahapiet and Ghoshal's (1998) model, this study identifies practical approaches that are used by threat modelling workshop facilitators to create conditions for effective knowledge exchange and combination. This study provides both cyber security scholars and professionals with an example on how to use knowledge creation related academic theories to analyse and further enhance cyber security risk management approaches by creating a connection between Nahapiet and Ghoshal's (1998) social capital model and cyber security threat modelling.

Keywords: social capital, knowledge creation, cyber security, workshop, threat modelling

1. Introduction

Organisational cyber security management focuses on protecting organisations' intellectual capital (Sallos et al, 2019). Threat modelling is a widely used approach for understanding cyber security related risks within existing and new software systems as well as the decisions made throughout the end-to-end software development lifecycle. The objective of threat modelling is to "analyse the potential attacks or threats to a system in a given context" (Uzunov & Fernandez, 2014, 734). The intended outcome of threat modelling is to establish a jointly agreed view on threats and their mitigation between participants (Shostack, 2014).

Successful threat modelling combines knowledge of the system's technical characteristics with an understanding of the security-related issues these characteristics and their implementation may generate (Uzunov & Fernandez, 2014). To support knowledge creation in threat modelling, various methods and guidelines have been created for teams and organisations (Uzunov and Fernandez, 2014). Some threat modelling methods and guidelines also help to identify the parties who possess relevant knowledge, and to facilitate knowledge sharing between different participants (Shostack, 2014). Knowledge exchange between different threat modelling participants can be supported for example by a dedicated facilitator who possesses understanding of the relevant threat modelling methods and guidelines (Ingalsbe et al, 2008).

However, identifying and involving relevant people in threat modelling activities or asking them to share their knowledge does not guarantee that adequate-level knowledge exchange takes place. Shostack (2014) mentions that the intended contributors may not want to share their knowledge, as they might for example feel strong ownership of the software they have created or might be concerned that threat modelling outcomes may increase their workload. To successfully model potential threats and attacks, organisations thereby also need to motivate and encourage knowledge sharing throughout threat modelling activities (Shostack, 2014).

While threat modelling methods and guidelines help to ensure that the most important aspects of threat identification and mitigation are covered, they seldomly address the social side of threat modelling activities, let alone the challenges that may prevent contributors from exchanging knowledge or agreeing upon the suggested mitigation activities. Yet, large number of stakeholders and their personal views and beliefs, together with other factors, such as political dynamics, create complexity that need to be considered when discussing cyber security knowledge management (Tisdale, 2015).

Sallos et al (2019, 592) suggest that "Cybersecurity-relevant organisational knowledge <…> is a function of the structure-mediated interactions between actors, their beliefs and the environment, which serve as a source of adaptation/calibration for further behaviour". This approach to knowledge is at the core of knowledge management research; knowledge is dynamic and evolves through continuous social interaction (Nonaka, 1994; Cook & Brown, 1999). An essential question is whether existing research on social aspects of knowledge creation can offer valuable insight that could be used to enrich cyber security related methods and approaches, such as cyber security threat modelling.

The objective for this research is to experiment whether the existing knowledge management research, more specifically the model describing the role of social capital in knowledge creation (Nahapiet & Ghoshal, 1998) could be used to understand the social aspects of knowledge creation in threat modelling workshops. First, the theoretical underpinnings of knowledge creation and social capital are introduced. Second, the research methodology is described. After this, empirical results are presented and discussed, followed by research limitations and conclusive remarks.

2. Theoretical background

2.1 Knowledge creation and social interaction

New knowledge is created in social interaction through continuous knowledge exchange and combination (Nahapiet & Ghoshal, 1998). Knowledge is continuously evolving through human interaction, as individuals involved in this interaction interpret the acquired knowledge in the light of the knowledge they already possess (Nonaka, 1994; Cook & Brown, 1999). Through human interaction, tacit knowledge is converted to explicit format and vice versa on individual and collective levels, and between these levels (Nonaka, 1994).

Knowledge management literature links social interaction to knowledge creation in several ways. Gupta and Govindarajan (2000) present that human interaction is characterized by the social ecology/social system that people are part of, and that this social ecology either facilitates or hinders all knowledge processes, including knowledge creation. Bhatt (2001) distinguishes prerequisites and enablers of knowledge creation; while the prerequisites include motivation, inspiration, experimentation and pure chance, knowledge creation is enabled by culture, organisational coordination, and information technology. Nahapiet and Ghoshal (1998) state that social capital is an organisational prerequisite for knowledge exchange and combination, as it facilitates knowledge exchange and combination.

Organisations can support knowledge creation by providing feasible conditions for it to take place. Grant (1996) suggests that organisations can intentionally facilitate knowledge creation by using integration and coordination mechanisms, and that common organisational knowledge is also needed to ensure aggregation of new knowledge to existing knowledge. Nonaka et al. (2000) describe how, in addition to human interaction, knowledge creation requires knowledge assets, a shared context for interaction and knowledge exchange ("Ba"), and managers who proactively generate conditions for organisational knowledge creation. Nahapiet and Ghoshal (1998) discuss collective knowledge creation, describing how shared interpretation between contributors is both a prerequisite and an outcome of knowledge exchange and combination in social entities. Additionally, they describe the relationship between social capital and knowledge creation as a continuum: whereas social capital is a prerequisite for knowledge creation, the evolving knowledge also modifies social capital within organisations. (Nahapiet & Ghoshal, 1998).

Cyber security management involves various stakeholders (Tisdale, 2015). Sallos et al (2019) emphasize the continuously evolving nature of cyber security related knowledge. According to them, organisations need to have a shared interpretation of this knowledge to support their cyber security related activities (Sallos et al, 2019). This thinking appears to be in line with the views of Nahapiet and Ghoshal (1998). What would then make Nahapiet and Ghoshal's model suitable for analysing knowledge creation in the context of threat modelling workshops?

2.2 Social capital and knowledge creation according to Nahapiet & Ghoshal (1998)

In their article "Social Capital, Intellectual Capital, and the Organisational Advantage", Nahapiet and Ghoshal (1998) suggest that social capital can both facilitate and inhibit generation of feasible conditions for knowledge creation in organisations. They state that all individuals and organisations possess social capital, consisting of networks of relationships and assets related to these networks, and identify three interlinked dimensions for

social capital in organisations based on previous literature: 1) *Structural dimension* that contains all network ties between actors, the qualities of different linkages and connections (network configuration) and how they are used (appropriable organisation); 2) *Relational dimension* that focuses on assets that are observable in personal relationships, such as trust, norms, obligations and identification, and that are forming the behaviour in organisations; and 3) *Cognitive dimension* that includes enablers, such as shared codes, language, and narratives that are required for creating a shared interpretation between actors. (Nahapiet & Ghoshal, 1998)

Nahapiet and Ghoshal (1998) also suggest that certain conditions need to exist before knowledge creation can take place. First, to be able to get engaged in knowledge creation, parties need to have an opportunity to do so, and this requires an access to potential sources of knowledge. Second, to get involved in knowledge exchange and combination, parties also need to anticipate some value from these activities. Third, they need to be motivated to get engaged in knowledge exchange and combination. These three conditions, *access to knowledge*, *anticipation of value*, and *motivation to create knowledge*, generate the momentum for knowledge creation. (Nahapiet & Ghoshal, 1998)

Three dimensions of social capital impact these three conditions in many ways. Structural dimension can either facilitate or hinder access to knowledge, as those aspects define the connections between different sources of knowledge. How these connections function in practice also impacts the anticipated value of parties involved in knowledge creation. The cognitive dimension (especially shared language and codes) may also facilitate or hinder access to knowledge, whereas the relational dimension, consisting of all the aspects embedded into personal relationships between people, may impact positively or negatively on all three conditions. (Nahapiet & Ghoshal, 1998)

In addition to having three conditions in place to create the momentum, parties involved in knowledge creation also need to be able to understand each other and to interact in terms of knowledge exchange and combination. Nahapiet and Ghoshal (1998) refer to this as the fourth condition, *combination capability*, describing the ability and means of the parties to exchange and combine knowledge while interacting with each other. Combination capability is strongly impacted by cognitive dimension of social capital; without shared language and codes, or shared narratives, the parties involved in knowledge creation lack means for both knowledge exchange and combination. (Nahapiet & Ghoshal, 1998)

Collective knowledge creation and self-enhancing nature of both social capital and collective knowledge described by Nahapiet and Ghoshal appears to be in line with the characteristics of organisational cyber security knowledge introduced by Sallos et al (2019) and to some extent also Tisdale (2005). Threat modelling workshops are relying on collective knowledge creation and forming shared interpretations (Shostack, 2014). Based on these remarks, it was considered worthwhile to test Nahapiet and Ghoshal's model in the context of threat modelling workshops.

3. Methodology

3.1 Research design

Research approach was based on a qualitative inquiry, and the scope consisted of three cyber security threat modelling workshops which took place within an organisation that utilized threat modelling as part of their cyber security-related activities. Each workshop was treated as a separate case, enabling both an individual and comparative analysis (Creswell 2013). Workshops included in the scope were jointly selected with information security professionals that acted as facilitators for the workshops, hence, purposeful sampling (Patton 2016) was applied. For each case, the primary research material consisted of non-participatory workshop observations, workshop recordings and four semi-structured interviews (with average duration of 47 minutes): the facilitator and the case owner were interviewed separately before and after the session. Research data was then deductively analysed using Nahapiet and Ghoshal's model (1998).

3.2 Data gathering and analysis

The purpose of individual interviews was to find out how the interviewees would describe the success factors and challenges for the threat modelling workshop they were involved with. Semi-structured approach including open ended discussion themes was applied for this purpose (Swaminathan et al, 2018). Workshop recordings and the related transcriptions were used as descriptive documentation of the interaction between workshop participants during threat modelling, and they were enriched by non-participatory observations which enabled

making additional remarks from the observer perspective on how the interaction took place (Gold, 1958; Swaminathan et al, 2018).

All three workshops and twelve interviews were conducted online, which enabled recording the audio and manually transcribing the content afterwards for analysis purposes. In addition to recordings, workshop observations involved taking field notes. For analysis purposes, all the material was anonymized due to confidentiality requirements, and technical details of the workshops were generalized.

First round of data analysis was done applying an inductive logic to identify passages related to tools and practices that were used for enabling and facilitating knowledge exchange and combination. Four conditions of knowledge creation from Nahapiet and Ghoshal's model (1998) were then used to go through the coded data and categorized using the four conditions of knowledge creation. Finally, the same data was also analysed using Nahapiet and Ghoshal's three dimensions of social capital (1998) and then compared with the previous analysis to identify links between the dimensions and the four conditions for knowledge creation.

4. Results and discussion

4.1 Results

Case organisation is a global software company with 1500+ employees. The company has a separate team of cyber security professionals to support other teams in their cyber security related activities, including threat modelling. Many of the company's software development teams do threat modelling as an integral part of their software development lifecycle, and threat modelling is also utilized by teams responsible for running the company's business operations. Empirical research material was collected from three separate threat modelling workshops (Workshops A, B and C).

Arrangements for all three workshop seemingly followed the same pattern: 1) A need for threat modelling was identified and recorded into work management system (WMS) using a work ticket; 2) Work ticket was analysed and a decision was made to contact security team for support (instead of doing threat modelling without support), and security team dedicated a facilitator for the workshop; 3) Scope, objectives, approach and participants for the workshop were agreed between the owner and the facilitator, and preparations were made; 4) The workshop was conducted; 5) Actions agreed during the workshop were recorded into WMS using work tickets, and other workshop outcomes (visualizations and notes) were included in the original work ticket.

Workshop facilitator and owner were jointly responsible for workshop preparations. As part of this, they agreed on the threat modelling scope and objectives, identified the participants needed for the workshop and selected the methods and tools to be used in the workshop. For all three cases, the method selected for threat modelling was STRIDE, originally developed at Microsoft Corporation (see, e.g., Shostack 2014), and the tools agreed to be used were data flow diagrams (for visualizing the scope and discussing the potential threats), Microsoft Teams (as a virtual meeting platform) and WMS (for sharing the documentation).

The workshops followed a four-step structure: 1) introducing the approach (including the objectives, scope, methods to be used and roles during the workshop), 2) drawing a description of the selected scope, 3) identifying threats related to the selected scope, and 4) summarizing the discussion. However, the emphasis of these steps varied based on the objectives and scope of each of workshop. During data gathering, it also became obvious that the three workshops selected for the research were different not only in terms of their context and scope, but also in terms of how well their objectives were met.

The person initiating Workshop A managed a third-party solution that the case company used for business management purposes. His team had been planning to start using threat modelling on a continuous basis during their solution management lifecycle, and they had contacted the security team for support. As a result, it had been agreed that a facilitated threat modelling workshop should be arranged to explain and showcase threat modelling methodology and approach for the team. Team lead assumed the owner role and based on the input from his team proposed selected functionalities to be threat modelled. It was decided that the whole team should participate in the workshop. During the 121-minute workshop, all five participants were actively contributing. Some of the tasks identified in the workshop required additional clarifications, and the owner took responsibility for these. It was also agreed between the owner and the facilitator that the facilitator would

continue supporting the solution team until they are comfortable with running their own threat modelling activities.

Preparations for Workshop B had started based on a change request initiated by an R&D team member who had been working with two different third-party solutions. In the change request, R&D team had suggested to add a direct interface between the two solutions. As a response for this request, teams managing these solutions had suggested using a facilitated threat modelling workshop to understand the impacts of the suggested change, and it was agreed that the R&D team lead would act as an owner for this workshop. After several meetings with various stakeholders, the facilitator proposed involving members from three separate teams: the R&D team and the teams managing the two third-party solutions. All three teams were able to decide their own participants, and during the 108-minute workshop, eight participants (40%) of the total twenty were actively participating. The outcome of the workshop was that the suggested change was even larger than first anticipated, and more thorough analysis should be conducted, as the changes would also impact on other teams than those who were represented in the workshop. Due to this, it was agreed that the facilitator would coordinate taking the discussion forward with all the relevant stakeholders.

Workshop C had been initiated by a software development team that normally did threat modelling on continuous basis but wanted to arrange a one-time workshop as they needed a facilitator to support them to understand a new interface. The team had a dedicated quality lead who acted as an owner for the workshop, while the team's product manager remained responsible for prioritizing and managing all activities arising from the workshop. All nine participants were from the same team, and during the 85-minute workshop, five participants (56%) were actively participating in the discussions. Based on the post-workshop interviews with the facilitator and the owner, workshop objectives were fulfilled, and follow-up was agreed to be done by the initiating team.

4.2 Observations regarding four conditions of knowledge exchange and combination

4.2.1 Access to knowledge

Without access to knowledge, the opportunity for knowledge creation does not exist (Nahapiet and Ghoshal, 1998). Individuals participating in threat modelling workshops seem to "bring their own knowledge" with them. Hence, identifying the right set of participants to be able to cover the selected scope appears to be crucial. Access to knowledge via participants was not an issue in Workshop C, and while few clarifications arose during Workshop A, those were not considered significant. In Workshop B, the participants did not possess all the required knowledge, and the objectives set for the work were not achieved. Based on the interviews, most threats are linked to such interfaces where technical or responsibility-related boundaries are crossed. Facilitators seemed to have wide knowledge on the company's overall technical architecture and potential threats within different types of interfaces, and they used this knowledge to identify relevant participants for the workshops.

4.2.2 Anticipation of value and motivation to contribute

People do not get involved in knowledge exchange and combination unless they anticipate that certain value is embedded in the interaction, and unless they are motivated to contribute (Nahapiet & Ghoshal, 1998). In each workshop, different factors seemed to impact how the participants got involved into the discussions. Workshop A facilitator and owner considered that the high activity rate (100%) was a result of the team's willingness to start threat modelling on a continuous basis to improve the security of their solution. This indicates that they anticipated value out of threat modelling activities and were motivated to get involved in reaching their goal of improving the security for their solution. Workshop B facilitator explained how a representative of one of the teams had forwarded the workshop invitation to additional people without anyone knowing, and that these additional participants attended the workshop just out of curiosity. Based on this they did not anticipate any value from contributing. Workshop C owner said that the inactive participants were not familiar with the new functionality and were attending only to educate themselves on the topic, meaning that they were there to receive rather than to create knowledge. Workshop C facilitator also mentioned that those participants who were responsible for the functionality in scope were the ones contributing, as they wanted to ensure that adding this functionality does not impact the overall product quality, which indicates they had high value expectations and high motivation to contribute.

4.2.3 Combination capability

Knowledge exchange and combination also requires combination capability that ensures that the parties can interact with each other (Nahapiet & Ghoshal, 1998). Regarding this research, this would mean the ability of participants to understand the selected scope on a required level and to be able to identify and mitigate the related threats. Based on workshop observations and interviews, facilitators were continuously enabling this by ensuring that shared language and codes were used. They selected the suitable methods and tools for the context in question based on their prior experience, and in each workshop, they first introduced these methods and tools and then continued by asking several clarifying questions to ensure the aspects of the selected approach were covered. They also seemed to know who would possess relevant information on each of the topics discussed and addressed some of the questions directly to these participants. In addition to this, they continuously explained why they were asking such questions.

4.3 The role of three dimensions of social capital in threat modelling workshops

4.3.1 The role of structural dimension

Structural dimension of social capital refers to the organisational patterns of connections, such as network ties, network configuration and the appropriability of the organisation, and it generates conditions to access knowledge, but also impacts the value anticipated from knowledge creation (Nahapiet & Ghoshal, 1998). Structural dimension had an observable impact especially on access to knowledge. First, it seems that established ties need to exist between the security team supporting threat modelling activities and the teams whose work is analysed for threat modelling purposes, and the quality of these connections seems to be important for such collaboration to succeed. Second, those who are responsible for the quality of threat modelling outcomes need to understand both the organisational and technical structure and related responsibilities to identify what kind of knowledge is required for threat modelling and where to get this knowledge. This includes the ability to identify the participants for the workshops as well as having access to these participants. This is also linked to organisational appropriability, as threat modelling may require establishing temporary connections across organisational boundaries in those cases where cross-team participation is needed (such as in Workshop B). Third, to ensure the condition for anticipated value is in place, the workshop initiators need to understand what the participants expect to achieve by participating in the workshop. Workshops B and C included participants who seemed more interested in gaining information and understanding how things work, rather than getting involved in identifying threats.

4.3.2 The role of relational dimension

Relational dimension of social capital drives access to parties but also anticipation of value and motivation (Nahapiet & Ghoshal 1998). Both the active participation during the workshops and the role of the facilitators as “trusted advisors” can be interpreted as signs of trust. On the other hand, they may also reflect the established norms of the organisation in question; the organisation seems to have rather established practices for threat modelling and cyber security management in general. Participant activity may also be linked to individual obligations; the active participants seemed somewhat obliged to contribute, as if they were automatically expected by fellow participants to express their opinions and insights.

4.3.3 The role of cognitive dimension

Cognitive dimension of social capital impacts on combination capability, and it includes resources that provide shared representations, interpretations, and meanings among parties (Nahapiet & Ghoshal, 1998). In all three workshops, methods, tools, facilitation, and documentation seemed to represent such resources. The workshop itself acted as a shared context for the participants, who were working towards a shared objective. Nahapiet and Ghoshal (1998) also point out the self-enhancing nature of social capital: when knowledge is created, it also further enhances all dimensions of social capital. Reflecting on this, threat modelling workshops can be viewed as part of knowledge creation continuum within the organisation; the collective knowledge created in the workshops contributed to both individual and collective knowledge within the case organisation.

4.4 Research limitations

Workshop observations and interviews produced plenty of material, but as Nahapiet and Ghoshal’s model was not used for steering the data gathering nor introduced to research participants, using it in a deductive manner included a risk of making wrong conclusions based on the available research material. To avoid this risk, only those parts of the data that were clearly referring to the elements in Nahapiet and Ghoshal’s model were included in the analysis. To avoid this in the future, the selected model should be used deductively from the

beginning of the research. Otherwise, the selected model seemed to suit well for qualitative inquiry; considering that Nahapiet and Ghoshal's model was introduced only after the research data had been collected, the way the model is structured helped categorizing the data and thereby fitting it into the model.

5. Conclusions

The objective of this research was to experiment whether collective knowledge creation in cyber security threat modelling workshops could be better understood with the help of Nahapiet and Ghoshal's (1998) model of social capital. Additionally, the intention was to evaluate, whether the selected model could be used to identify additional ways to support social interaction within the context of threat modelling. For this purpose, three threat modelling workshops were observed, and the owners and facilitators of these three workshops were interviewed before and after the workshops.

In their model, Nahapiet and Ghoshal (1998) focus on describing collective knowledge creation and shared interpretations. They also propose that social capital impacts on the conditions for knowledge creation, and that organisations can modify their social capital to promote feasible conditions for knowledge creation. Based on this research, the existence of these conditions, the approaches and practices facilitating these conditions as well as the impact of social capital were observable during threat modelling workshops and the related preparation and follow-up activities. In case the model would be used for similar purposes in the future, using the model deductively from the beginning of the research should be considered. Additionally, a follow-up inquiry with the organisation using this model to analyse their threat modelling practices would help understand whether the results have been useful.

References

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

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, pp 381–400.

Creswell, J. W. (2013) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches,* SAGE, Thousand Oaks, CA.

Gupta, A.K. & Govindarajan, V. (2000) "Knowledge Management's Social Dimension: Lessons From Nucor Steel", *MIT Sloan Management Review*, Vol 42, No. 1, pp 71-80.

Ingalsbe, J.A., Kunimatsu, L., Baeten, T. & Mead, N.R. (2008) "Threat Modeling: Diving into the Deep End*", IEEE Software*, January/February, pp 28-34.

Nahapiet, J. & Ghoshal, S. (1998) "Social Capital, Intellectual Capital and the Organizational Advantage", *Academy of Management Review*, Vol 23, No. 2, pp 242-266.

Nonaka, I. (1994) "A Dynamic Theory of Organizational Knowledge Creation", *Organization Science*, Vol 5, No. 1, pp 14-37.

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

Patton, M. Q. (2016) *Qualitative Research and Evaluation Methods*, SAGE, London.

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, pp 581-597.

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

Swaminathan, R. & Mulvihill, T.M. (2018). *Teaching Qualitative Research. Strategies for engaging emerging scholars*, The Guilford Press, New York, NY.

Tisdale, S. M. (2015) "Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective", *Issues in Information Systems*, Vol 16, Issue III, pp 191-198.

Uzunov, A.V. & Fernandez, E.B. (2014) "An extensible pattern-based library and taxonomy of security threats for distributed systems", *Computer Standards & Interfaces*, Vol 36, pp 734–747