Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share

Christian Sillaber[1], Clemens Sauerwein[1], Andrea Mussmann[1], and Ruth Breu[1]

[1] Universität Innsbruck, Department of Computer Science, Innsbruck, Austria
{firstname.lastname}@uibk.ac.at

Abstract. An increasing interest in Cyber Threat Intelligence (CTI) sharing platforms can be observed in research and practice. The main purpose of these platforms is to support the automated sharing, evaluation and dissemination of CTI, as well as the creation of inter-organizational sharing communities. Unfortunately, little is known about the added value these platforms provide to organizations as innovation in this area is mostly driven by vendors, and empirical studies are rare. In order to understand how these platforms provide value to organizations, we conducted a case study consisting of an exploratory survey and two focus group discussions with 17 stakeholders currently seeking to implement such a platform. The main goal of our research was to identify stakeholders' key expectations and types of information they are willing to share on a prospective CTI sharing platform. Building on these results, we propose a maturity model for CTI sharing platforms.

Keywords: Cyber Threat Intelligence Sharing, Threat Intelligence Data, Information Sharing, Case Study, Maturity Model

1 Introduction

In the past, organizations used ad-hoc solutions such as email, phone calls, or face-to-face meetings to disseminate cyber security-related information. Recently, a trend to form interconnected communities within and across organizational boundaries to manually and automatically exchange cyber security related information (e.g. Indicators of Compromise) can be observed [1-3]. As a reaction to this trend, software vendors and governmental institutions started to create offerings that facilitate this exchange and appear under the umbrella term *Cyber Threat Intelligence (CTI) Sharing Platforms* [4, 5]. For example, the government of the Netherlands has introduced a national detection, response, and expertise network [6], NATO has initiated the Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) project [7], and the Computer Incident Response Center Luxembourg (CIRCL) has developed the Malware Information Sharing Platform (MISP) [8]. Additionally, several standardization efforts (e.g. STIX, TAXII) to support automated CTI sharing gained traction in recent years [9-11]. Moreover, research and practice have shown that this type of exchange

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

presents a potential countermeasure against today's sophisticated cyberattacks, as not every organization has the resources to develop an adequate security program independently, and organizations can benefit from other organizations' experiences [3, 12, 13].

Today's commercial and non-commercial CTI sharing platforms embody three fundamental concepts to a greater or lesser degree: (a) Facilitate information sharing, (b) enable automation, (c) facilitate the generation, refinement and vetting of data through burden-sharing collaboration or outsourcing [1, 5, 7]. Unfortunately, little is known about the added value these platforms provide as empirical research in this area is almost non-existent and innovation is driven by vendors and technological trends [14]. Moreover, research in recent years has focused on fundamental concepts of CTI sharing platforms [7,15,16] without analyzing the value they provide. As a first step towards closing this gap, we seek to answer the following research question: *What are the capabilities and functionalities of CTI sharing platforms and what is the nature of provided CTI and different levels of maturity?* The goal of our research was therefore to investigate the expectations of stakeholders, especially early adopters, of CTI sharing platforms. Special focus was put on the specific artifacts that are shared and the participants' willingness to share them. Based on these investigations, a maturity model for CTI platforms was derived. This model can be used to measure the maturity and provided value of CTI sharing platforms to stakeholders and organizations.

The case study consisted of a series of focus group discussions and interviews with 17 stakeholders from 17 organizations that are planning to introduce a joint CTI sharing platform. The stakeholders represent 17 globally operating organizations and either directly work in their organization's security operations center or are the organization's chief information officer or chief information security officer.

Our research has shown that stakeholders of CTI sharing platforms expect the platforms to have automated sharing functionalities that facilitate the timely sharing of quantitative and qualitative CTI between participating organizations. Additionally, the platform should offer functionalities to control the information flow and provide trust metrics. In order to provide a comprehensive solution and increase the value of CTI sharing platforms for organizations, stakeholders emphasized the need of integrating external information sources, like vendor specific security advisories or mailing lists. Finally, based on these findings we introduced a model to measure the maturity of CTI sharing. The remainder of this paper is structured as follows. Section 2 provides related work regarding CTI sharing platforms and related studies. Section 3 outlines the underlying research methodology and procedure carried out. Section 4 presents the key findings. Section 5 discusses the results and derives a maturity model to evaluate the maturity level of CTI sharing platforms. Finally, section 6 concludes the paper and provides an outlook on future research.

2 Related work

Dandurand and Serrano were the first who formulated 11 high-level requirements for CTI sharing platforms [7]. Since then, several researchers identified further requirements and challenges for CTI sharing [1, 7, 15, 16]. Moreover, several author

introduced concepts or frameworks for cyber security information sharing [17, 18]. For example, in [17] the authors propose evolving procedures for organizations to advance and improve their cyber security information sharing maturity. However, none of these publications are based on empirical investigations. In addition, several efforts have been made to standardize CTI (e.g. STIX, TAXII, Open IOC) [9, 10, 19]. In 2016, for example, the National Institute of Standards and Technologies (NIST) published an official guide to cyber threat information sharing which is based more or less on these standardization efforts [11]. However, all these contributions introduce high level requirements without taking into consideration the individual stakeholders' expectations and reservations for such platforms.

Only a few empirical studies in the domain of CTI sharing can be identified. In [1], the requirements for a holistic CTI sharing platform based on a study of several market solutions are discussed. In prior work we discuss data quality challenges and future research directions in CTI sharing practice based on focus group interviews with security experts [14]. Murdoch and Leaver provide a case study on the UK government's cyber security information sharing partnerships and arising anonymity and trust issues [20]. Bhatia et al. conducted a survey of 76 security professionals in order to analyze the privacy risk and fears in cyber security data sharing across organizational boundaries [21]. Sauerwein et al. provided a comprehensive analysis and comparison of open and closed source inter-organizational CTI sharing platforms [5].

Maturity models have been proposed by researchers and practitioners across multiple domains to assist organizations with transformations or the introduction of new technologies [22]. By identifying predictable evolutionary stages, maturity models help describe anticipated or desired steps from an initial state of capabilities to a mature state of capabilities of a specific application domain [22, 23].

To the best of our knowledge, no prior empirical research has been conducted that takes into consideration the maturity and value of CTI sharing platforms based on stakeholders' expectations and their willingness to share CTI. Additionally, none of the aforementioned contributions introduces a model to measure the maturity and value of CTI sharing platforms.

3 Research Methodology

We conducted a case study with members of a security expert group developing a national CTI sharing platform in a central European country. The case study consisted of two parts that were conducted during the first half of 2016. At first, we conducted an exploratory survey which formed the basis of our subsequent focus group discussions and interviews. In order to ensure reproducibility, a research protocol was developed which consists of filled out questionnaires, survey results, workshop transcripts, and a list of participants. Following the basic design principles for maturity models, as proposed in [22], we limited the application domain of the maturity model to inter-organizational CTI sharing platforms. As the maturity model was developed in close collaboration with expert matter stakeholders, aforementioned documentation of interviews and discussions serves as documentation of the design process.

3.1 Participants of the Case Study

The case study was conducted with 17 domain experts from industry. Table 1 gives an overview of the participants, their roles, and the types of organization they are belonging to. The majority of participants work in major financial organizations. While all companies operate globally, one of them is small (<150 employees), four of them are medium (150-1000 employees), and 12 of them are large-sized organizations with more than 1000 employees each. Moreover, the composition of participants represents a mixture between employees that work directly in their organization's security operations center (e.g. security analysts) and persons who are members of the managerial level (e.g. chief information security officers). Finally, it is worth mentioning that four participants already use a threat intelligence sharing platform at their organization.

3.2 Explorative Survey

In order to reduce the possibilities of omitting important concepts and artifacts from our case study, we conducted an exploratory survey as a pre-study ([24, 25]). As part of this survey, the participants (see Table 1) were asked to state their expectations and requirements for a CTI sharing platform from the perspective of their role and organization's security operation center's processes. In addition, the participants were asked to specify what type of information and intelligence they are willing to share with other participants of such a platform. To bootstrap the thinking, we provided participants with an initial list of potential information and intelligence artifacts. This list was based on the "data types and elements of interest to members of the security operations team" presented in [11]. The participants were asked to classify the elements of the list based on the Traffic Light Protocol (TLP)[1], where elements can be marked as red (R), amber (A), green (G) or white (W). The color assigned to an information element defines how it may be shared within the CTI sharing platform. For example, information which is marked as red cannot be shared with any party outside of the original group of people the information provider chose to share it with. If an information element is marked as green, it can be shared with all participating organizations. The results of this survey were analyzed and formed the basis for the subsequent focus group discussions.

3.3 Focus Group Discussions

After analyzing the results of the exploratory survey, two focus group discussions [26] were conducted. The participants were the same as in the exploratory survey. The goal of the focus group discussions was to gain deeper insights in the stakeholders' valuation of CTI sharing platforms. Discussion topics were the stakeholders' expectations for such a platform, their willingness to share information, and the classification of information they are willing to share. The two focus group discussions were held in parallel at a neutral premise in 2016 and lasted roughly one and a half hour each. The

[1] 1https://www.us-cert.gov/tlp (Accessed: September 19th, 2017)

aim of these parallel discussions was to limit bias from other participants and get more meaningful results by cross-comparing the results. Before the two discussions started, all 17 participants were instructed by two researchers. Afterwards, two discussion groups were formed randomly, where each group consisted of eight to nine participants and one moderator. Every moderator was a researcher with expert knowledge in the field of CTI sharing platforms. Researchers asked questions during the discussions to clarify participants' statements and to refocus the discussion. Each workshop was recorded and transcribed. After the workshops, qualitative summaries were produced from the recordings [27] in order to derive the findings relevant to the research [28].

Table 1: Overview of the participants of the two focus group discussions.

ID	Organizational Role	Type of Org.	# of Employees	Use TISP
1	Security Analyst	Finance	> 1000	
2	Security Architect	IT	150-1000	X
3	Secuirty Analyst	Finance	> 1000	
4	Security Researcher	Education	< 150	X
5	CERT Member	Production	150-1000	X
6	Security Specialist	Finance	> 1000	
7	Security Task Force	Finance	150-1000	X
8	CSIRT Member	Finance	> 1000	
9	SOC Team Leader	-	< 150	
10	CISO	Insurance	> 1000	
11	CISO	Finance	> 1000	
12	CISO	Finance	> 1000	
13	Security Analyst	Finance	> 1000	
14	MSSP	IT	> 1000	
15	Head of SOC	Finance	> 1000	
16	Security Specialist	Finance	150-1000	
17	Security Consultant	Consulting	> 1000	

4 Study Results

From the analysis of the exploratory survey and focus group discussions, we gained insights into stakeholders' expectations and willingness to share information on a threat intelligence sharing platform. In the following section, we discuss them in detail.

Expectation 1: CTI sharing platforms must reach a critical mass. The interviewees stated that a critical success factor of a CTI sharing platform is the number of participating organizations and contributing branches from industry. In this context, nearly 80% of the interviewees agreed that they expect at least a certain number of participants within a platform which belong to their branch of industry and are located in their country. For example, the majority of study participants belonged to the financial sector and therefore it is not surprising that they primarily expected a certain number of financial institutions in their prospective CTI sharing platform. However, interviewees were not able to quantify the critical number of participants they expect. The remaining 20% of interviewees stated that they expect the participation of large and medium-sized organizations and a good mixture of business, academic and

governmental institutions. While we were not able to obtain quantifiable numbers either, these 20% of interviewees agreed that as many organizations as possible should participate.

Expectation 2: The shared CTI should be more current than conventional information sources and reduce the time to detect threats. All interviewees agreed that they expect the timely supply of actionable information in order to stay up-to-date regarding occurring threats and incidents. They assume that the necessary information can be obtained in real-time, is not outdated and is more current than information from conventional sources like vulnerability or exploit databases. Accordingly, they see great potential to reduce time to detect cyber threats and instantiate countermeasures more timely.

Expectation 3: A CTI sharing platform should offer social media and automated sharing functionalities. Nearly half of the interviewees stated that they expect social media functionalities. For example, they expect features similar to group chats, news streams, dashboards or forums. In this context, two interviewees remarked that a CTI sharing platform should be more a social media platform for information security experts than a data warehouse holding tons of e.g. indicators of compromise. They expect a lively community that shares indicators of compromise for emerging threats enriched with the collective knowledge and experiences of the participating experts. Moreover, five interviewees stated that they expect fast, easy to use and automated sharing capabilities. In this context, two interviewees mentioned that a notification feature regarding new threats or incidents would be desirable.

Expectation 4: CTI sharing platforms should implement functionalities to control what is shared with whom. Using the information from the interviews and the surveys we found that potential users expect control of information exchange and filtering of the received information. The interviewees emphasized that they attach importance on control mechanisms to guarantee the exchange of information with trustworthy participants and capabilities for anonymization or pseudonymization. They want to choose one-to-one or one-to-many information exchange depending on the sensitivity of information. For example, one interviewee stated that he wants to share information regarding a cyber attack with all participants of a platform if his organization is not directly targeted, but keep it confidential if required. In this context, one interviewee made the point that in this case it would be helpful to provide a functionality which enables anonymous sharing of information. Moreover, the interviewees emphasized the need for filtering and subscription functionalities. By using these functionalities, users of a CTI sharing platform can control the information flow and counteract information overload. For example, one participant of the workshops stated that too much information provided by such a platform would result in a lot of additional work to identify information relevant to a company and diminish the value of receiving the right information in time. The interviewees emphasized that functionality to filter for most serious attacks, industry, company size, region or country would be useful. In this context, four interviewees expected that a CTI sharing platform only delivers information which matches with their organization's infrastructure. For example, a company uses only operating system A, then the platform should provide all CTI regarding A and omit information regarding operating system B, which is not used.

Expectation 5: CTI sharing platforms should integrate external information sources. Half of the interviewees stated that they rely on external information sources, such as mailing lists, as part of their daily information security processes. Since they expect that a CTI sharing platform should be an all-encompassing information source to support their processes they emphasized the need of integrating external information sources. Information sources of interest are vulnerability databases, information security mailing list, exploit databases, information security expert blogs, vendor specific security advisories, bug repositories, malware and virus databases. Moreover, one interviewee suggested to establish connections to other CTI sharing platforms and support the information exchange with them. The interviewees reasoned that these external information sources would enrich existing CTI and would provide new security information for a CTI sharing platform.

Expectation 6: Stakeholders expect qualitative as well as quantitative information from a CTI sharing platform. During the workshops, a debate was sparked by the participants' different opinions about the nature of CTI. On the one hand, about 60% of the participants stated that they mainly expect quantitative information or rather technical information from a CTI sharing platform. For example, malicious URLs, malware samples, malicious IP addresses, file hashes, phishing emails or malicious email addresses. On the other hand, nearly 40% of the participants expect qualitative information from a threat intelligence sharing platform. They assume that plain technical information regarding threats can be derived from other information sources while such a platform provides qualitative threat intelligence based on knowledge sharing between organizations. From the interviewees' perspective, qualitative CTI consists of technical information regarding threats enriched with contextual information, and knowledge of other participating organizations. Moreover, qualitative information expands organizational knowledge based on experiences from other organizations, increases the interpret-ability of technical information and provides support for the implementation of proper countermeasures to handle specific threats.

4.1 Stakeholders' willingness to share CTI

The interviewees were asked to classify the information elements according to the respective categories of the Traffic Light Protocol (TLP) [11]: Red, Amber, Green, White and Anonymous. Red and Amber mark limited disclosure and restricted to members of the information exchange. Red is stricter and limits the access to representatives participating in the information exchange which have signed certain rules. Green means that information can be shared with all participating organizations on a CTI sharing platform and White means that the information is intended for public and unrestricted dissemination. Last but not least, Anonymous means that information can be publicly disclosed in an anonymized form. We found that the majority of information sharing elements of interest are marked with Red or Amber which means that stakeholders are willing to share this type of information merely in closed groups where they know each participating organization. During the workshops they argued that the unintentional disclosure of CTI to unknown third party organizations might damage the organization's reputation and put its business at risk. For example, one

interviewee stated that if his organization publicly discloses information about an encountered information leak it might harm the trust relationships with their customers. Another workshop participant added that it might not be beneficial if every competitor on the market is informed about an encountered attack since the competitors can use it to strengthen their market position and harm their competitor. In this context, the interviewees emphasized the need for mechanisms to control with whom the information is shared (c.f. Expectation 4). Moreover, our research showed that the interviewees are willing to share malware samples and artifacts with all participating organizations on a CTI sharing platform. This is understandable as malware samples and artifacts are not necessarily tied to the organization that found it. Few information elements were classified as "White', which means that the information is publicly available to everyone on the platform. This is not surprising since the participants of the study assumed that their prospective CTI sharing platform is closed to organizations within their security expert group. Hence, the platforms do not plan to provide access to third party organizations outside their community. Finally, the interviewees showed willingness to share some information in anonymized form; for example, SMTP headers, emails, captured packets, IP addresses or domain names, or any other information artifact potentially containing personal identifying information. During the workshops, we investigated this phenomenon in detail and the interviewees stated that they are willing to share these elements but they want to avoid traceability. For example, organization A shares the content of an Email of a phishing campaign. Then organization A does not want any other participating organization within the platform to trace it back to them.

5 Discussion

In the following Section we introduce a maturity model based on the results of the explorative survey and the focus group discussions. In addition, we provide a discussion on the limitations of the methodology used to conduct the research.

5.1 Towards a maturity model for CTI sharing platforms

Based on the focus group discussions, and analysis of literature in the field of CTI sharing, we developed a maturity model for CTI sharing platforms. This descriptive maturity model [23] can be used by organizations as a guiding framework to assess the maturity level of their CTI sharing efforts and to move to higher levels of maturity in a systematic and incremental way. Although the maturity model is developed mainly based on data from European financial organization, we believe that it can be used by government agencies or organizations from other domains without major modifications because the core principles and objectives of CTI sharing are the same. The maturity model is depicted in Figure 1. As an organization's CTI sharing effort moves to a higher maturity level, the organization's stakeholders are more engaged and the systems are better connected, thus a greater value for the organization is realized. However, a higher maturity level faces increased complexity and interdependencies which may lead to

greater challenges and risks. Based on the analysis of the CTI sharing platform market presented in [5], we conclude that most CTI sharing platforms cover maturity levels three and four. While we believe that, in principle, an organization should move sequentially through the proposed stages from the lowest to the highest maturity level, a combination of process improvement and adequate tool support will help organizations to "leapfrog" one or more maturity levels at once. By focusing on reaching one maturity level at a time, organizations can effectively build infrastructure, capabilities and knowledge without integrating complex software and joining large sharing communities all at once.

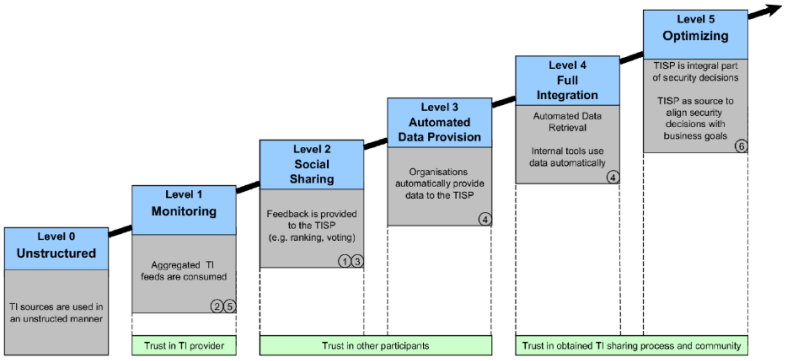

Figure 1: Maturity model for inter-organizational CTI (TI) sharing. (Remark: The numbers in the circles are referencing the respective expectations.)

Level 0: Unstructured Level 0 of the maturity model refers to an initial stage, where no or only some open CTI sources are used in an unstructured and unsystematic manner. A level 0 organization focuses primarily on reactive security and risk management activities and passively consuming information without contributing to the platform. It lacks a centralized, structured approach to collecting and organizing incoming CTI. A typical level 0 organization would have some members of the security and risk team subscribing to mostly technical newsletter, bulletin boards, etc. The utilization of this intelligence largely depends on the personal processes and willingness to share of some individuals.

Level 1: Monitoring: Level 1 represents the first step towards CTI sharing. Organizations at this level have a centralized CTI aggregator that collects incoming information for all team members (c.f. Expectation 5). The interaction is one way, but the organization disseminates the incoming intelligence in a structured way and reacts accordingly. Organizations that have reached this level have an advantage over those that manually collect, filter and process intelligence from conventional information sources and can therefore reduce the time to detect cyber threats (c.f. Expectation 2).

Level 2: Social Sharing: Organizations that have reached level 2 actively participate in an exchange with their peers. Incoming intelligence is disseminated, evaluated and manual feedback is provided through social media functions through e.g. sharing, voting or message based discussions (c.f. Expectation 3) with other participants of the platform. This increased dependency on other participants' feedback requires organizations at this level to trust other participants and the provided data. As

knowledge sharing platforms require a certain number of participants to leverage network effects (c.f. Expectation 1), a full realization of all benefits from level 2 requires a lot of effort.

Level 3: Automated Data Provision: Organizations at level 3 share some of their internal data automatically with the community and directly connect to the CTI sharing platform. For example, manually reported phishing emails or virus alerts are automatically transmitted to and disseminated through the platform. As this requires a high level of trust in the other participants, granular control over what is shared with whom is required. For example, CTI sharing platforms at this level allow organizations to define sharing groups or sharing rules based on e.g. the TLP (c.f. Expectation 4).

Level 4: Full Integration: At level 4, organizations already trust both the data provided by the platform as well as other participants. At this level, organizations integrate some components of their security landscape into the CTI sharing platform to benefit from automation. For example, firewall rules are automatically updated to block suspicions traffic and spam filters automatically include shared rules to detect phishing emails, spam and emails containing viruses. As this requires organizations to select specific subsets of intelligence streams, a granular control over the intelligence flow is required (c.f. Expectation 4).

Level 5: Optimizing: Level 5 indicates that real-time CTI, shared (semi-) automatically, is an integral part of an organization's security and risk management processes. Real-time qualitative and quantitative intelligence is a foundational part of aligning security and risk management decisions with business goals (c.f. Expectation 6). A level 5 organization puts in place an effective governance structure and process to enable continuous improvement and innovation of security and risk management programs. Furthermore, organizations and governmental bodies, and other stakeholders form and nurture a mutually beneficial continuous ecosystem cycle for effective security and risk management through high quality CTI.

5.2 Limitations

Our case study might be limited by certain threats to validity. As described in [29] the application of focus group discussions in empirical research might be limited by certain threats to validity. Limitations that have to be acknowledged and accounted for are a (i) selection bias when selecting the participants for the case study, (ii) influences of moderators during the focus group discussions, (iii) off-topic discussions, (iv) language barriers and (v) an incomplete or biased list of CTI sharing elements stakeholders are willing to share.

In order to counteract limitation (i) to (iv) we followed the suggestions by Vogt et al. [30]. According to them, (i) participants of the case study were asked to participate voluntarily, (ii) moderators tried to keep in the background as much as possible, (iii) moderators refocused the discussion as soon as it got off track, and (iv) the explorative survey and focus group discussions were held in English. To counteract (v), we used the "data types and elements of interest to security operations personnel", presented in [11]. Moreover, the participants had the possibility to extend the list of sharing elements.

6 Conclusion

As organizations adapt to today's cyber threat landscape by leveraging the knowledge and capabilities of multiple organizations to curb advanced cyber threats, the usage of CTI sharing platforms has gained traction to coordinate these efforts. An extensive analysis of stakeholders' expectations and willingness to share through a series of interviews and focus group discussion indicates that different maturity levels of CTI sharing platforms exist. We propose that, by moving from one maturity level to the next level in an orderly manner, organizations can avoid unnecessary risks, build their CTI sharing capabilities systematically, and enable a systematic approach to collecting, analyzing and reacting to CTI. Although we have developed our model with a focused group of expert stakeholders and several interviews, future research needs to validate our model more rigorously using quantitative empirical data. In addition, our model is largely based on these organizations' perspectives and future research can improve the model by incorporating a more holistic community perspective. We acknowledge that there are situations in which the linear progression of our proposed maturity model is not practical and an organization can benefit from skipping one or more levels. We believe that our model will serve as an initial step to engage researchers and practitioners in ongoing conversations to further leverage the promised values of CTI sharing platforms.

Acknowledgements: This work was partially supported by the Austrian Federal Ministry of Science, Research and Economics (BMWFW), FFG Project 855383 SALSA (ICT of the Future).

References

1. S. Brown, J. Gommers, and O. Serrano, "From cyber security information sharing to threat management," in Proceedings of the 2nd ACM WISCS, ACM, 2015, pp. 43–49.
2. F. Fransen, A. Smulders, and R. Kerkdijk, "Cyber security information exchange to gain insight into the effects of cyber threats and incidents," Elektrotechnik und Informationstechnik, vol. 132(2) pp. 106–112, 2015.
3. S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," Information Management & Computer Security, vol. 22, no. 5, pp. 410–430, 2014.
4. F. Skopik, G. Settanni, and R. Fiedler, "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," Computers & Security, vol. 60, pp. 154–176, 2016.
5. C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives," in 13. Internationale Tagung Wirtschaftsinformatik, WI 2017, St.Gallen, Switzerland.
6. E. V. D. Heuvel and G. K. Baltink, "Coordination and cooperation in cyber network defense: the dutch efforts to prevent and respond," Best Practices in Computer Network Defense: Incident Detection and Response, vol. 35, p. 121, 2014.
7. L. Dandurand and O. S. Serrano, "Towards improved cyber security information sharing," in Cyber Conflict (CyCon), 2013 5th International Conference on. IEEE, 2013, pp. 1–16.
8. C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in Proceedings of the Workshop on Information Sharing and Collaborative Security. ACM, 2016, pp. 49–56.

9. P. Kampanakis, “Security automation and threat information-sharing options,” Security & Privacy, IEEE, vol. 12, no. 5, pp. 42–51, 2014.
10. J. Steinberger, A. Sperotto, M. Golling, and H. Baier, “How to exchange security events? overview and evaluation of formats and protocols,” in Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015, pp. 261–269.
11. C. Johnson, L. Bager, D. Waltermire, J. Snyder, and C. Skorupka, “NIST special publication 800-150: Guide to cyber threat information sharing,”, NIST, Tech. Rep., 2016.
12. S. Ernest Chang and C.-S. Lin, “Exploring organizational culture for information security management,” Industrial Management & Data Systems, vol. 107, no. 3, pp. 438–458, 2007.
13. Ponemon, “The value of threat intelligence: A study of North American & United Kingdom companies,” Ponemon Institute LLC, Tech. Rep., 2016.
14. C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, “Data quality challenges and future research directions in threat intelligence sharing practice,” in Proceedings of the 2016 ACM WISCS. ACM, 2016, pp. 65–70.
15. O. Serrano, L. Dandurand, and S. Brown, “On the design of a cyber security data sharing system,” in Proceedings of the 2014 ACM WISCS. ACM, 2014, pp. 61–69.
16. S. Appala, N. Cam-Winget, D. McGrew, and J. Verma, “An actionable threat intelligence system using a publish-subscribe communications model,” in Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. ACM, 2015, pp. 61–70.
17. W. Zhao and G. White, “An evolution roadmap for community cyber security information sharing maturity model,” in Proceedings of the 50th HICCS Conference, 2017.
18. M. A. Alhawamdeh, “Developing a conceptual national information sharing security framework to combat cybercrimes in jordan,” in CCSCloud, 2017 IEEE 4th International Conference on. IEEE, 2017, pp. 344–350.
19. R. A. Martin, “Making security measurable and manageable,” in Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008, pp. 1-9.
20. S. Murdoch and N. Leaver, “Anonymity vs. trust in cyber-security collaboration,” in Proceedings of the 2nd WISCS Workshop. ACM, 2015, pp. 27–29.
21. J. Bhatia, T. D. Breaux, L. Friedberg, H. Hibshi, and D. Smullen, “Privacy risk in cybersecurity data sharing,” in Proceedings of the 2016 WISCS. ACM, 2016, pp. 57–64.
22. J. Pöppelbuß and M. Röglinger, “What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management.” in ECIS, 2011.
23. T. De Bruin, R. Freeze, U. Kaulkarni, and M. Rosemann, “Understanding the main phases of developing a maturity assessment model,” 2005.
24. E. R. Babbie, Survey research methods. Cengage Learning, 1990.
25. S. L. Pfleeger, “Experimental design and analysis in software engineering,” Annals of Software Engineering, vol. 1, no. 1, pp. 219–253, 1995.
26. S. Wilkinson, Qualitative research: Theory, method and practice, Cengage Learning, 2004.
27. P. Mayring and M. Gläser-Zikuda, Die Qualitative Inhaltsanalyse. Beltz Weinheim, 2008.
28. J. L. Campbell, C. Quincy, J. Osserman, and O. K. Pedersen, “Coding in-depth semi structured interviews problems of unitization and intercoder reliability and agreement,” Sociological Methods & Research, 2013.
29. K. Louise Barriball and A. While, “Collecting data using a semi-structured interview: a discussion paper,” Journal of advanced nursing, vol. 19, no. 2, pp. 328–335, 1994.
30. D. S. Vogt, D. W. King, and L. A. King, “Focus groups in psychological assessment: enhancing content validity by consulting members of the target population.” Psychological assessment, vol. 16, no. 3, p. 231, 2004.