Sharing Communities: The Good, the Bad, and the Ugly

Thomas Geras*
HM Munich University of Applied Sciences
Munich, Germany
thomas.geras@hm.edu

Thomas Schreck*
HM Munich University of Applied Sciences
Munich, Germany
thomas.schreck@hm.edu

ABSTRACT

There are many mysteries surrounding sharing communities, mainly due to their hidden workings and the complexity of joining. Nevertheless, these communities are critical to the security ecosystem, so a more profound understanding is necessary. In addition, they face challenges such as building trust, communicating effectively, and addressing social problems.

This work aims to understand better the working methods, organizational structures, goals, benefits, and challenges of sharing communities to help improve their effectiveness and efficiency. To achieve this goal, we conducted video interviews with 25 experts from different countries worldwide who participate in various types of sharing communities. In addition, we applied socio-technical systems (STS) theory in our analysis process to elaborate on our findings from the interviews, identify correlations between them, and explore the interrelationships between social and technical elements of sharing communities.

Our findings underscore the need for a holistic view of how sharing communities work. Instead of looking at individual aspects in isolation, considering the interrelationships between the different elements, especially the social, is crucial. This holistic perspective allows us to understand better the complexity and dynamics of sharing communities and how they can function effectively and efficiently. The findings of this study provide valuable impetus for the further development of sharing communities and can serve as a basis for future research.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; **Economics of security and privacy**.

KEYWORDS

cyber threat intelligence; information sharing; sharing communities; csirt; socio-technical systems theory; social and technical aspects

ACM Reference Format:
Thomas Geras and Thomas Schreck. 2023. Sharing Communities: The Good, the Bad, and the Ugly. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3576915.3623144

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11.
https://doi.org/10.1145/3576915.3623144

1 INTRODUCTION

During the last three decades of handling large-scale attacks, one crucial part was sharing information between stakeholders. In 1988, the outbreak of an Internet worm called "Morris Worm" [24] showed no coordination during the attack against multiple targets. The following year the "CERT/CC" was founded in Pittsburgh by the direction of DARPA [12]. In 1990, during the next incident with global impact - the "Wank worm" - it became obvious that exchange between security teams was necessary. One problem was that no explicit team was responsible for coordinating the measures against the attack, but many organizations connected to the Internet had their own security team. That led to the creation of the first sharing community called the "Forum of Incident Response and Security Teams" (FIRST) [10].

An effective response to cybersecurity threats often requires collaboration and information sharing among individuals and organizations with different interests and expertise. One example of such collaboration was forming the "Conficker Working Group" during the 2008 outbreak of the "Conficker worm" [19]. Through daily communication and joint efforts, the working group members could share important information about the malware's behavior and collaborate on mitigation strategies. This coordinated response allowed for faster deployment of patches and updates to prevent further damage. Overall, the success of the "Conficker Working Group" demonstrates the importance of collaboration and information sharing in responding to cybersecurity threats and mitigating their impact.

The sharing communities mentioned earlier are just a few examples among many, each with unique missions and self-conceptions. A sharing community is a collective of individuals who prioritize cooperation and mutual support, sharing resources and expertise to help meet each other's needs. For example, some sharing communities focus on facilitating team collaboration to exchange incident data or share best practices efficiently. In contrast, others are built on trust among individuals, with the expectation that each member will contribute to the overall security of the Internet. In summary, sharing communities can take various forms and serve different purposes. Still, they all aim to promote collaboration, trust, and reciprocity in addressing cybersecurity threats and promoting a more secure and resilient digital ecosystem. Further examples of sharing communities besides FIRST are the Cyber Defence Alliance (CDA), Cyber Security Sharing & Analytics (CSSA), and Financial Services Information Sharing and Analysis Center (FS-ISAC).

Sharing communities have become increasingly complex in several dimensions. Exploring them is proving difficult because many of these groups operate behind closed doors, and joining is challenging. Therefore, we conducted video interviews with experts from different countries who are members of various sharing groups. With this knowledge, we can better understand the organizational

structures, goals, benefits, and challenges of different types of sharing groups. We applied STS theory in our analysis process to gain a more comprehensive understanding of these aspects and identify the interrelationships between them. This allowed us to deepen our analysis and holistic understanding of sharing groups, their social and technical elements, and their interrelationships. In this way, better recommendations can be made to improve the effectiveness and performance of sharing communities. Through this study, we aim to help current sharing communities better understand themselves and use our work to improve their day-to-day operations and foster a positive change process.

To our knowledge, we are the first to analyze organizational structures, goals, benefits, and challenges of sharing communities. In addition, this study provides a foundation for a better understanding of the complex functionality, structures, and interrelated social and technical elements of sharing communities. It is a first step toward applying socio-technical systems theory in this context. In this study, we will answer the following research questions:

RQ1: [Structures] *What organizational structures are established in sharing communities?*
RQ2: [Goals & Benefits] *What goals and benefits do members see from information sharing and participation in a sharing community?*
RQ3: [Challenges] *What are the challenges in sharing communities?*

We used an exploratory research approach to understand this under-researched topic comprehensively. To do this, we developed the interview questions based on the research gaps, and the research questions crystallized, evolved, and refined as the research project progressed. In summary, we make the following contributions:

- We analyze the organizational structures in sharing communities, including types, member profiles, tools, community size, and member maturity.
- We identify the benefits for members of sharing and participation in sharing communities.
- We recognize the prevailing goals and challenges in sharing communities to develop targeted approaches and strategies for more effective collaboration in the future.
- We deepen the understanding of sharing communities by thoroughly examining and analyzing the social and technical elements and their interactions through the STS theory.
- We present optimizations for key findings to promote a collaborative and information sharing experience.
- Our multi-layered analysis of sharing communities allows to better understand the complexity of these groups and the factors that influence the effectiveness and efficiency of collaboration and information sharing.

The remaining paper is structured as follows: We discuss related work in Section 2, then we describe our methodology in Section 3, followed by our findings of the interviews in Section 4. We use STS theory to deepen our findings and investigate the social and technical elements of sharing communities in Section 5. Subsequently, we discuss our work and provide recommendations for future research in Section 6. Finally, we conclude our work in Section 7.

2 RELATED WORK

In this section, we highlight the relationships and distinctions between our work and existing research in the field of sharing communities. In addition, we describe the underlying theory of our analysis process.

2.1 Sharing Communities

In our research, we examine the various aspects of sharing communities and apply socio-technical systems theory to analyze them further. No previous work has used this approach to study and understand the social and technical elements and their interactions within a sharing community. However, prior work has concentrated on current challenges in sharing Cyber Threat Intelligence (CTI) and how to improve it. Wagner et al. [26] analyzed a large amount of literature regarding information sharing. The main objective of their research was to identify challenges related to automating the process of sharing CTI. They divided their investigation into three major categories: (1) CTI sharing, (2) Actionable CTI, and (3) CTI sharing regulations. Within each category, they identified key aspects and challenges. While their research focused primarily on the technical aspects of sharing and a specific sharing mission, there were some overlapping conclusions with our work.

Zibak and Simpson conducted various online studies and literature reviews regarding sharing communities. They first conducted an online survey to understand the gaps between theory and practice within information sharing [28]. Their findings indicate that sharing information positively impacts the overall security posture. However, they also identified several barriers to effective sharing, which can hinder its effectiveness. Further, they analyzed the influence of sharing on the various stakeholders, especially on security analysts [27, 29]. They introduced a study method and analyzed various aspects of CTI sharing. The study proposed a categorization framework for different types of information sharing and identified issues related to evaluating the effectiveness of sharing efforts.

Kollars et al. [15] investigated the rapid rise of Information Sharing and Analysis Centers in the US. Bouwman et al. [1] conducted an extensive study about commercial Threat Intelligence Sharing platforms. The study analyzed two paid CTI vendors and found that their indicators had a low overlap, even for specific threat actors. There is little sharing of indicators across vendors, and paid information promise to overcome the problem of sharing threat information among defenders has not been fulfilled. Recently Bouwman et al. [2] measured the impact of one large sharing community, the "COVID-19 Cyber Threat Coalition" (CTC), and found out that this sharing community provides added value. By pooling data, the CTC improved coverage of COVID-19-related threats faster than other defenses for listing such domains. However, over time, the CTC lost focus and aggregated mostly generic abuse information due to scaling up its quality assurance processes using VirusTotal.

2.2 Socio-Technical Systems Theory

The work of Davis et al. [9] builds an essential foundation for explaining and applying STS theory to sharing communities in our paper. Complex systems consist of multiple elements often interacting simultaneously in various ways [6]. According to the STS framework of Davis et al., shown in Figure 1, any complex

organizational system can be represented as a hexagon with the following six elements: goals, people, culture, infrastructure, technology, processes, and procedures. The first three mentioned are the social or human elements, and the last three are the technical elements. Furthermore, the system is embedded within an outer frame, including a regulatory framework, financial or economic factors, and stakeholders. However, the relevance and impact of those external factors will vary depending on the system [7]. According to Leavitt [20] and Cherns [5], all these elements, both social and technical elements, must be considered jointly to promote positive change [9]. Additionally, due to the complex nature of these systems, changes in one element will affect other elements, and the overall effectiveness of a STS is limited if changes are only considered in one element and not other elements [7, 9].

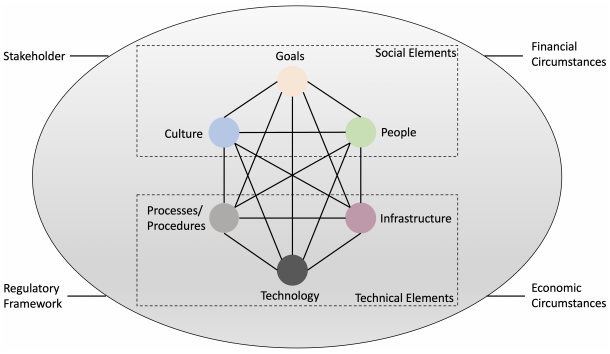

Figure 1: Socio-technical system by Davis et al. [9].

The STS framework of Davis et al. enables representing, analyzing, and understanding complex systems and their interrelated social and technical elements in a simple, structured, systematic, but powerful manner. Moreover, STS thinking promotes identifying relationships, potential conflicts, or gaps between various system components (e.g., culture and goals) to encourage the development of systematic recommendations and improvements and foster positive change [4, 9]. According to Johnson et al. [13], studying complex systems consisting of multiple interacting elements at different levels of hierarchy is ideally suited for applying STS.

Sharing communities have social and technical components and can therefore be viewed as complex organizational systems within the STS approach. We see several advantages of analyzing sharing communities with the STS framework: It enables structured and systematic analysis, deeper understanding, and better representation, ultimately leading to improved collaboration and information sharing within communities. Another advantage of the STS framework is that it presents and makes understandable the elements and interactions of a sharing community, both individually and collectively. The goal is to go beyond the social and technical elements to gain a holistic view of the complex system, leading to sound analytical conclusions and practice-relevant insights.

3 METHODOLOGY

We conducted 25 semi-structured video interviews with CTI experts from different countries who have been members of various sharing communities for many years to understand the complex organizational structures, goals, benefits, and challenges of sharing communities. In addition, we applied STS theory in the analysis process to investigate the interrelationships between them and to research the social and technical elements as well as their interaction. In the following, we describe the individual steps of our research project.

3.1 Preparation

Ethical consideration. At the beginning of our research, we used a self-assessment form provided by our institution to review the ethical aspects of our research. Based on this, approval from the ethics committee was not required. An inquiry to our ethics board further confirmed this. To avoid NDA violations by the interviewees, we focused on the general experiences and findings of the interviewees.

Experts. When selecting the experts, we emphasized the sufficient professional experience of at least five years in CTI. Another requirement was membership in several different sharing communities. To ensure a diverse perspective, the experts should come from different industries, fields of work, and countries. Through these inclusion criteria, we can assume that the expert developed a more comprehensive and practical understanding of the topic and provided valuable, diverse insights for our research. Other factors such as gender, socioeconomic or employment status did not affect the selection. Access to the experts was primarily based on long-standing relationships, and the contact was made by email.

Questionnaire. We created a semi-structured interview guide using the SPSS (collect, check, sort, and subsume) method [11]. The findings presented in this paper are part of a broader data collection effort to understand better sharing communities and quality management within these groups. For this reason, our interviews were designed in four parts: (1) Demographics, (2) Sharing communities, (3) CTI & quality management, and (4) Related challenges. The selection of the interview questions was motivated by the identified research gaps and the significant role of sharing communities in cyber defense, as no previous research has examined the operational processes, organizational structures, and challenges of sharing communities. Our interview questions' focus helped us fill existing gaps and provide new insights into this vital area.

Testing questionnaire. We conducted two evaluation steps to ensure that the interview guide met scientific standards and the quality of social experiments. In the first step, we evaluated the interview guide regarding question order, wording, and clarity with an expert in political science and interview methodology. In the second step, we reviewed the questionnaire with two CTI experts. Based on their feedback and referring to Kruse and Schmieder [16], we improved the questionnaire regarding usefulness, wording, terminology, and comprehensibility. In addition, this step checked whether some questions were unspecific, ambiguous, or led to undesired answers. The final questionnaire can be found in Appendix B.

Informed consent. Before the interviews, experts were informed about the study objectives, scope, recording, and anonymization, transcription, and data handling procedures. Participation was voluntary, and the experts were informed about the possibility of withdrawing from the study at any time. We obtained a signed

informed consent in advance of the interviews. In addition, verbal consent was obtained before the audio recordings began.

3.2 Data collection

Sample size. Our sample size was guided primarily by the principle of data saturation [3] and the recommendations of Marshall et al., who suggest a sample size between 20 and 30 participants [22]. In our case, we found that the insights and themes we obtained were consistent and recurrent, suggesting that we had reached data saturation at 25 interviews. In addition, our sample size was sufficient to provide a comprehensive understanding of the research topic while ensuring the trustworthiness and validity of our findings.

Interview conduct. The interviews were conducted between May 25 and August 30, 2022. All video interviews were conducted by the same interviewer and with an institutional instance of Zoom [30]. At the beginning of the interviews, we presented two definitions to ensure a common understanding of sharing communities and CTI (see Appendix B). By doing so, we ensured that both the interviewer and the interviewee shared the same understanding of critical aspects of the research topic. We then asked questions based on the interview guide but also discussed topics that arose spontaneously. The interviews ranged from 20 to 105 minutes, with an average duration of 53 minutes.

3.3 Data handling

Transcription. Subsequently, the audio files of the recorded interviews were used to create the non-verbatim transcripts using Adobe Premium Pro [21]. The tool works offline and does not upload the audio files or the finished transcripts. In the following, we manually anonymized all personal information that allowed inferences about the interviewees as part of the transcription process according to Kuckartz [17]. At the same time, we manually corrected errors in the transcript when matching it to the audio file. After completing the transcripts, we allowed the interviewees to review the transcript for accuracy, as suggested in [8]. However, we emphasized that changing the interpretation of the transcript was not allowed. By allowing the interviewees to review the transcript, we wanted to increase the trustworthiness, validity, and accuracy of the transcript. Furthermore, we wanted to ensure that anonymization was adequate. As a result, we corrected some minor grammatical errors or incorrect words in the transcript.

Data protection. The personal data of the interviewees were stored locally under password protection. The audio files and the transcripts were stored anonymously on an institutional instance of GitLab, to which only the authors of this study had access. By storing the personal data separately from the interview data, the risk that conclusions could be drawn about the interviewees was minimized.

3.4 Analysis

Content analysis. We analyzed the collected data with thematic content analysis according to Kuckartz [18]. In this systematic and structured procedure, the existing text material is analyzed material-as well as rule-guided. Our analysis process included the following steps: (1) Highlighting notable passages in the transcribed text and recording special features, (2) Deriving main categories from guiding questions and available material and creating a coding plan, (3) Coding the text and placing it in the appropriate category, (4) Creation subcategories, (5) Re-coding the entire material with main and subcategories, (6) Compilation of all coded text passages per main and subcategory, (7) Evaluation and presentation of the results in visual form, which can be seen in Appendix C. The results of this analysis step can be seen in Section 4.

Socio-technical systems theory. Subsequently, we further analyzed the results from Section 4 following Davis et al. [9]. We performed the following steps: (1) Examine and rank data, (2) Determine and group key system elements and visualize, (3) Evaluate the importance of the external environment, (4) Consider relationships between elements, (5) Review and assess under-explored or related areas of the hexagon framework visually, (6) Complement additional factors that arise from the data, (7) Review the analysis with one key stakeholder for accuracy, possible errors, and interpretations, and modify as necessary after consultation, (8) Draw essential conclusions about the system and how it works. The results can be seen in Section 5.

3.5 Limitations

Due to the conduction of expert interviews, self-reporting or response bias is challenging to prevent. Therefore, experts could be influenced by the interviewer, questionnaire, or the online environment during the interview. In this context, three interviewees conducted the interview without turning on the camera. In addition, interviewees could answer socially desirable and give biased responses. Finally, it should be noted that our all-male sample, although unintentional, may limit perspectives in the data and affect the generalizability of the results.

Other potential limitations could arise from our approach of applying socio-technical systems theory. For example, our study analyzes sharing communities in general as a socio-technical system, but studying a specific sharing community could lead to different results. Moreover, sharing communities are subject to constant change, and our approach presents only a subjective interpretation at a particular time.

4 FINDINGS

In this section, we use the input of the 25 expert interviews to address our research questions, outlined in Section 1. The interviews helped us to gain a detailed perspective into the various types of sharing communities and, therefore, to answer these questions.

4.1 Demographics

The experts who participated in the interviews have extensive and diverse experience in dedicated security teams, national CERTs, and large enterprises. Some experts have several decades of professional experience and were present in the early days of sharing communities. A detailed account of the important aspects of the demographics for this study can be found in the Appendix A, with work experience in years and the order randomized.

At the time of the interviews, the experts were working in the following countries: United States of America (6), Germany (6), Great Britain (3), Netherlands (3), Australia, Poland, Luxembourg, Thailand, Greece, Switzerland, and Brazil.

4.2 RQ1: Structures

In this section, we answer **RQ1:** *What organizational structures are established in sharing communities?* Here, we investigate the different types of sharing communities, the members and their roles, the collaboration, and the impact of the size and maturity of members.

4.2.1 Types of Sharing Communities. Sharing communities may differ in admission rules and level of formality and may also be topic- or region-specific. Below, we describe the types of sharing communities we identified in the interviews.

Open sharing communities. Those groups usually come without entry rules or NDAs and are open to the general public. They can be non-formal and self-governed by members of a community or formal and governed by CTI vendors who built open sharing communities around their services or tools. In these open groups, data is usually shared, not CTI. Therefore, the type of group also impacts the value and quality of the information shared.

Closed sharing communities. In comparison, closed sharing communities have strict access rules for new members. Well-known closed sharing communities include the Cyber Defense Alliance, Cyber Security Sharing & Analytics, FIRST, or ISAC. Some of them are fee-based and based on legal frameworks or NDAs. These clearly define what may be shared, how, and with whom. In some circumstances, sharing is even mandatory. These sharing communities are known to be very professional and trustworthy. Therefore, they are also called trust communities and contain more valuable CTI than open communities. As communities grow, more and more unknown members join, leading to a loss of trust. Therefore, "vetting" or "vouching" communities have been created. To become a new member of these "hidden clubs" a member must propose an applicant. After that, the other members vote on or vet the applicant, or a member must even vouch for the applicant.

Topic- or incident-related sharing communities. Another type of group, which can be open and closed, is very specific in its goal and formed only for a particular topic or incident by members who already know and trust each other. They are short-lived and will be closed after the incident is solved. One can think of them as a task force of specific experts.

4.2.2 Members in Sharing Communities. To better understand the composition and the cooperation within a sharing community, it is necessary to understand who the members are.

Membership structure. The interviewees identified researchers, analysts, engineers, corporate executives, and management staff as potential sharing community members. They may participate as individuals or representatives of organizations such as CSIRTs, PSIRTs, CERTs, law enforcement agencies, governments, ISPs, and friendly military organizations. Participation varies by community combination. Only very few interviewees indicated that they know their stakeholders and constituencies well. However, these interviewees emphasized that this would facilitate collaboration and exchange of CTI. In this regard, the majority of interviewees indicated that it is typically not possible to generalize and define who a member is. Often, it is not even possible to identify specific individuals.

Desired membership profile. We also discussed with the interviewees which members should be represented in a sharing community for the interviewees to achieve their goals by participating in a sharing community. Most interviewees emphasized the importance of a similar maturity level among members, leading to shared challenges and similar skills. However, a different level of maturity is not a barrier to sharing. Some interviewees cited membership composition as important: three interviewees preferred diversity to increase visibility, and two preferred members from similar sectors or areas that combat similar threat actors. In contrast to the above statements, four interviewees emphasized the importance of member characteristics such as willingness to build trust, share CTI or knowledge, and provide feedback. In addition, two interviewees mentioned specific roles as important members, such as an administrator or "critical master" who begins sharing, "ideally two or three different members", as an incentive for other members to "build up a culture of sharing".

4.2.3 Roles in Sharing Communities. In addition to the general information about members mentioned above, it is critical to understand the roles in which members participate in sharing communities. In the following, we describe the most frequently mentioned roles.

Producer or sources of CTI. Everyone who can produce, generate, collect, aggregate, and share it within the community might be considered a producer or source of CTI.

Consumer of CTI. These are members who consume the shared CTI for different application areas. Besides consuming, the consumer role can also provide feedback or add context to the producer or source of CTI. Moreover, a consumer can act as a producer and source of CTI. However, in the eyes of one interviewee, consumers generally do not have the proper capabilities to act as producers and therefore share less valuable information that is false and burdensome to the group. Nonetheless, some consumers act as producers to feel more a part of the sharing community.

Sharing enabler. A sharing enabler is critical for representatives of an organization who are not sharing on behalf of their name. The important aspect of this role is that it gives the representatives permission to share. In addition, the sharing enabler provides financial, human, and time resources and support.

Broker, middleman, or proxy role. This role acts passively by exchanging and collecting CTI from multiple places or entities, forwarding it to the proper entity, or filtering it for a specific sharing community. Moreover, this role can also act actively and perform various analyses, add context, and enrich CTI, so it can better be utilized. Some of these tasks are performed by CERTs, for example. This role can also serve as an anonymizer for certain entities that do not want to communicate with each other or be recognized.

Host. The host, administrator, or group organizer takes over all organizational tasks. For example, this role brings people together, contacts members, and organizes meetings or events, as FIRST does.

Lurkers or leechers. Lurkers or leechers do not share and only consume CTI or observe the sharing community, also called "free rider" [25]. One interviewee explained that there are always different degrees of maturity in a sharing community, and everybody starts as a leecher.

4.2.4 Collaboration. Tools and platforms are essential for collaboration and sharing between members. For example, communication between members is achieved through ad hoc conversations in Slack channels, Signal, Telegram or WhatsApp groups, Discord, Zoom, or mailing lists. One interviewee pointed out that "90 percent of the conversations are held in Slack", and channels have up to 1000 members. The exchange of CTI usually happens through mailing lists, Threat Intelligence Platforms (TIPs), or shared repositories. The most used TIP was the Malware Information Sharing Platform (MISP) [23]. Some of the interviewees are members of ISACs, and, therefore, mostly use self-developed platforms specifically designed for their use case.

In addition to tools for communication and sharing, tools such as JIRA and Confluence are used for collection, and Dropbox or GitHub are used for sharing CTI. One respondent said that these tools are excellent for people who do not have access to TIPs. In addition, Twitter was also cited as an excellent source for CTI because it is quick to share, and one can reach many people.

4.2.5 Size of Sharing Communities. In the interviews, we talked about the scalability of sharing communities. Only a few interviewees were clear about whether a sharing community can scale. Three interviewees reported positive experiences in groups with 100 and even 1000 members, suggesting that a large sharing community can be effective. Another interviewee added that sharing communities can scale as long as there is a legal framework and members understand the general conditions.

In this context, different positive aspects of larger groups were mentioned. For example, the greater diversity of members in a large community can positively influence members' capabilities, who start "copycatting" processes and procedures of more mature members. Furthermore, larger communities allow for reaching more members, which can be suitable for specific use cases and goals. Nevertheless, there is also a risk that threat actors can learn about the efforts of large and prominent communities, gain access to this information, and use it to adapt their tactics, techniques, and procedures (TTPs) before they become unusable. In this context, one interviewee described the conflict of conscience between information sharing within small groups, which could lead to essential detections, and sharing within large groups, which could disrupt TTPs.

As we learned from the interviews, the overall sharing in large communities will diminish over time, leading to the "atrophy" of the group. Furthermore, the size also influences the shared information. The proportion of OSINT increases with the size of the community, although this will not lead to an increase in the quality of shared CTI. In contrast, CTI shared in smaller groups has more context and is more focused on something related to the own entity, and therefore has more value for the members. Usually, "sensitive information" and the "juicy stuff" is shared in groups with only a few members. Furthermore, smaller sharing communities are "leaner, more nimble, and you trust each other".

Trust is another aspect to keep in mind. As the sharing community grows, trust within the community becomes more difficult. Five interviewees mentioned trust concerns. For two, scaling a group technically might be possible. However, the level of trust "scales inversely". One interviewee advocated for a maximum of 15 participants so that each member could bring an additional colleague and everyone fits at the same table, which promotes knowing each other and increasing trust.

4.2.6 Members Maturity. In sharing communities, there are usually "different levels of maturity in terms of CTI". At a certain level of maturity, members have clear processes and goals and understand why sharing or community work is necessary. Initially, new members begin with a leeching phase. As members mature, they begin to understand the importance of sharing back, engaging, providing feedback, and helping other members of the community. Although several interviewees emphasized the importance of maturity, they did not use a specific formula to determine the maturity level of members.

Nevertheless, based on their years of experience, the interviewees can estimate that usually very quickly, for example, through a combination of received data sets, collaboration, and conversations with these members. The maturity level with respect to sharing communities is reflected in aspects such as knowledge of handling confidential information or the willingness to provide feedback to other members on shared CTI. For one interviewee, even the amount of sharing is a matter of maturity rather than the size of the community, as described by other interviewees in the previous section.

4.3 RQ2: Goals and Benefits

We now present our findings for **RQ2:** *What goals and benefits do members see from information sharing and participation in a sharing community?*

4.3.1 Goals. The interviewees identified several goals they have in sharing CTI and participating in a sharing community. Six main types of goals emerged from the responses and are described below.

Supporting each other. This primarily altruistic goal was cited by eight interviewees. Sharing CTI in a sharing community allows people to help themselves, help other members, take appropriate action, and better defend themselves. Furthermore, this goal includes informing other members about current threats. Thus, giving and receiving early warnings to the community is a meaningful aspect of being in a sharing group.

Contribution to society. This goal was mentioned six times and can be described as a more idealistic and broader goal of CTI sharing, like "make the world a better place" and bringing threat actors to justice. This results in the goal of improving the security situation in the world. Like the first goal, this goal reflects that the common welfare is at the forefront for many members.

Understanding the threat landscape. Four interviewees aim to understand current threats, what exactly is happening, evaluate if and how vulnerable they are against current threats, and quantify the risk of becoming a victim of cyber attacks. Furthermore, tracking attackers' behavior was also named a vital goal.

Continuous defense adjustment. Based on the actual threat landscape, four interviewees highlighted the importance of adjusting and adapting their cyber defense to current threats and techniques.

Proactive threat mitigation. Includes protecting networks and individuals, detections, mitigating attack potential, and improving cyber defense. This goal was also mentioned four times by the interviewees.

Integration of others into sharing communities. One interviewee remarked that helping new people get into a sharing community and help them to build trust is very important. This is an interesting goal, especially in the context of the challenges related to trust groups we discuss in Section 4.4.

4.3.2 Benefits. The benefits of participating in a sharing community extend well beyond obtaining CTI and include several aspects that benefit members. The most valuable benefits mentioned are described below.

Knowledge sharing. The most mentioned benefit of sharing communities is "knowledge sharing". This includes "access to people and access to information". Nine interviewees mentioned various forms of knowledge sharing, for example, sharing reports, scripts, solutions, and best practices related to defense procedures or automation, which all have high value and lead to saving resources. Moreover, the information gained through discussions, calls, and bilateral cooperation with sharing community members is a great advantage. For example, the information gained may be operational knowledge about hunting techniques, priorities, and other peers' work focus, such as observed threat actors or campaigns. In the process, one's own focus may shift to new events or unknown threats.

Visibility and warnings. Anything that improves visibility and awareness was cited by eight interviewees as a benefit of sharing communities. The collective capabilities promote visibility and quickly learning about and understanding new events.

Relationships. For six interviewees, the relationships that are built in sharing groups are of great importance. This includes meeting new people with different skills, building trusted relationships with peers, and the "bilateral collaboration". In addition, the various relationships allow problems to be escalated and an event to be viewed by multiple experts.

Receiving help and support. Once relationships are established and trust is built, six interviewees find it a great benefit to receive help and support. For example, to get help in emergencies or to have the ability to make all kinds of "broadcast requests" within the sharing community. However, this benefit is more pronounced in trust groups.

Resource savings. Another benefit related to relationships within a sharing community is that statements and information from trusted peers have more value and help save resources. Four interviewees pointed out the great benefit of work sharing in this context. For example, the enrichment of CTI is distributed to various parties with different visibility, or a finished report sometimes saves a "half working day".

Feedback and context. Three interviewees saw feedback and additional context as a significant benefit of a sharing community. They emphasized the importance of sightings in this context, as they provided them with a benchmark for shared CTI. One interviewee added that receiving feedback, for example, on quality, allows producers to have quality management passed on to consumers. In addition, receiving additional information about the shared CTI, its usefulness, recommended actions, and how to deal with specific CTI increases its applicability.

4.4 RQ3: Challenges

In this section, we answer **RQ3:** *What are the challenges in sharing communities?* Below, we describe the most relevant challenges facing sharing community members.

Low-quality CTI. High CTI quality is of "utmost" importance to all interviewees, and they can usually quickly identify poor quality when receiving it. However, poor CTI quality is a significant challenge in practice, especially for those who share low-quality CTI. Multiple interviewees mentioned that this could lead to being excluded from receiving sounder CTI, damaging reputation, or even being blocked. Furthermore, distributing low-quality CTI leads to losing customers and financial damage for CTI vendors since customers will not renew the services.

Two interviewees are very strict and will not maintain sharing relationships if a vetting process is missing or the quality is insufficient. According to one interviewee, quality requirements vary across communities, and these differences influence the importance and prioritization he assigns to groups. Although the quality of CTI is crucial, quantitatively expressing the quality is not trivial and lacks practical applications among the interviewees.

Missing context. "CTI is all about context". However, context is very subjective, and not everything important for one entity is relevant for another. Therefore, distinguishing or understanding between what is objective and what is subjective is a critical task. Context is crucial for various reasons, like knowing the purpose for receiving that given CTI, what to do with it, and what it means to specific consumers. Without this context, the challenge arises that many entities do not understand how certain CTI should be used to be effective.

Missing feedback. Feedback is desirable for many who share CTI but is often missing. Constructive feedback on shared information, such as sightings or additional insights, would increase quality and generate CTI in a more targeted manner. Any form of feedback is welcome, for example: Was it useful? Who was affected? Who has additional information? Who can confirm it? One interviewee noted that the feedback loop is mostly ad hoc or nonexistent and estimated that only 1 to 2 percent of his consumers provide feedback.

Amount of data and sharing communities. The data overload makes it challenging for members of sharing communities to filter and select relevant information. In addition, it is difficult to determine the appropriate number of memberships in sharing communities. People fear missing out and want to be in all groups because the exchange is spread across many communities. This makes it very difficult for the interviewees to keep track of everything. In this context, the question is, "how many relationships does one need?". One is probably not sufficient, and one hundred is probably too much. This information overload leads to overseeing the critical and valuable CTI. Instead, the majority of interviewees are drowning in mediocre and valueless CTI.

Work overload and mental health. The overload of information leads further to another challenge in the field - work overload and a burden on mental health. The work overload and pressure

of staying on top of what people are doing is a real threat and challenge to people's mental health. For example, a one-week vacation may cause the threat perception of one of the interviewees to change completely. Furthermore, the fluctuation in the field is high, so the same job is not executed for long. A survey of Kinsella [14] confirmed some of the aspects above related to work overload and mental health.

Lack of visibility. Despite the enormous flood of information, the lack of transparency of the threat landscape and specific threat actors is one of the biggest challenges, particularly regarding nation-state actors. The lack of visibility results from the absence of specific entities in the sharing communities. Some entities are underrepresented, like people from certain regions or companies. The lack of visibility was also named as one of the top five challenges in the survey of Kinsella [14].

Definitions, ontologies, standards, taxonomies. During the interviews, there were several in-depth discussions about individual challenges and problems with various technologies and standards at very detailed levels, for example, STIX, TAXII, or using the IDS flag. Most of the issues discussed were individual preferences rather than generalizations of problems. However, most of the standards developed in standardization committees are very detailed and often too complex for the daily work of an analyst. In addition, there are many different standards, taxonomies, and ontologies, which still makes consuming CTI very difficult. Even similar events from different sources cannot be compared. In summary, there is no standard between different sharing communities. This means that different sharing communities use different tools, platforms, taxonomies, and ontologies.

Lack of sharing. A challenge that threatens the existence of sharing groups is the lack of sharing. One interviewee stated that this had been a problem for a long time and concerned large sharing communities like FIRST or TF-CSIRT, where limited threat sharing occurs. There are many reasons for the lack of sharing, such as lack of trust or maturity, lack of incentives, or a "blame culture" in which "the one who shares" is "the first to get the blame". One participant highlighted the relevance of encouraging people to share, educating them, and showing them the need to share. However, a minority of the interviewees stated they experienced a lack of sharing within organizations due to legal constraints or a culture of fear. One interviewee said that the consequences of failure are much higher for him or his company than success through the shared CTI.

Lack of newcomer. One disadvantage of the vetting or vouching process is that the same people often come together in different trust communities. This became a major challenge during the COVID-19 pandemic. One expert stated that this made it "difficult to bring new people" and is one reason for the absence of newcomers. It is essential to be active in the field, to have a good reputation, or to know the right people. However, some people do not like attending conferences and prefer to remain unknown. "There is now a dilemma" because some groups are dying out. Suggesting people and vouching for them can also have consequences for the person who brought the new member into the community if the new member does not follow the rules.

Subgroups. A phenomenon in open and closed sharing communities is the formation of subgroups within a group. To become a subgroup member, engaging and being active in the community by sharing, responding, helping, and supporting is important. It is also important to know the right people. The reward will then be invited into a subgroup "where the action happens". Sometimes even in trust groups, subgroups or TLP red groups are created, and even the trust group members do not know those subgroups exist. One reason for forming subgroups is that people do not engage in large communities and have trust issues. Therefore, people form subgroups with active and qualified people they trust more. Other reasons for forming subgroups are regional or sector-specific, where there is more common ground. For example, based on MISP correlations.

Trust. Trust is a key component to the success of a sharing community, and the group can be an "anchor from which trust starts to be built". However, "trust is a human problem", and "it needs some effort to create that trust network" with strangers one has never met. In this context, one interviewee pointed out that he knows groups where people trust each other and have worked together for years even though they have never met. Though, for most interviewees, getting to know each other in person is important. Therefore, workshops, conferences, or evening events are fundamental for the interviewees. In addition, being active in sharing communities is very important for building trust. It signals to other members that someone is not only here to leech but also to give something back.

Recalling false data. False data in data sets is another mentioned challenge since it usually stays online forever. Thus, encouraging people to recall wrong and false data is a significant challenge. Hence, there should be ways to clean up or remove erroneous data as soon as one identifies it. Otherwise, it will affect businesses.

Missing guidance. When a sharing community grows, the number of less mature entities and OSINT increases. Therefore, these entities need guidance, like sharing and behavior rules. Unfortunately, this is usually lacking in sharing communities.

Commercialization. Another challenge for sharing communities is the commercial market, which sometimes stops building public communities. Several organizations will not participate in sharing communities because they consume information from vendors and do not see a benefit in sharing additional information.

5 SHARING COMMUNITIES AS A STS

In this section, we combine the previous section's insights with our perspective on sharing communities and apply them to the STS (see Section 2.2). In each subsection, we first explain the respective element. We then analyze the respective element based on the most critical factors and describe how these can be optimized through examples. At the end of each element, we give examples of its influence on the other elements of the system.

5.1 Goals

In sharing communities, goals are critical to members' and groups' success and collaboration. However, we learned from the interviews that members have very different goals (see Section 4.3). These goals may conflict with the goals of their organization and with the goals of the sharing community. Therefore, open communication about goals is essential to create a shared understanding of expectations and priorities within the group. In this way, members can align

their individual goals and create synergy. When goals conflict, compromise, and consensus are necessary to resolve these conflicts and maintain and improve collaboration.

Furthermore, flexibility and continuous adaptation of goals to the ever-changing threat landscape are essential. Therefore, the dynamics of goal setting should be coordinated in close collaboration with members regularly. In this context, goal evaluation and monitoring are critical to tracking the progress of sharing communities in achieving their goals. Regular evaluations and monitoring allow communities to ensure success and make timely adjustments. These suggestions can help increase the collaboration's effectiveness and improve member satisfaction.

Finally, goals influence other elements of sharing communities. Members' individual skills and resources can be better aligned with the community when members understand the goals and share the same objectives. A community with clear goals is more likely to develop a culture of collaboration and trust. Members who share the same vision work together to achieve goals. In addition, people within a group work more focused, motivated, and efficiently when goals exist towards which they are working.

Moreover, with clear goals, members can better develop common standards and best practices to define and optimize processes and procedures within a community. In addition, goals significantly influence the selection and development of technology and infrastructure. Finally, goals can help guide decisions about allocating resources, designing communication channels, and implementing supporting technologies.

5.2 People

People in a sharing community are the members who participate in different roles as individuals or representatives of an entity. In addition, some people, such as colleagues or family members, influence the group and benefit from it indirectly. In Section 4.2, we have pointed out that the composition, roles, and maturity of members, as well as the size of groups, vary and have different implications on the community. A thoughtful composition of members based on specific roles, skills, or characteristics can prevent problems such as lack of trust, limited sharing, or forming subgroups. Clearly defining and assigning roles in this context can help improve group collaboration and communication and ensure that resources are used effectively.

A changing composition of community members, roles, and skills can affect the group's performance. Therefore, it is crucial to have an overview of the members and their respective roles. This makes it easier for members to find the right group and for the group to be purposeful and adapt as needed. Since most community work is often voluntary and not mandatory, motivating members to get involved and participate in addition to their daily work is critical to the group's success. Therefore, members' needs and concerns should be addressed, and members should receive appreciation for the contributions that they deserve. Trust and social relationships are inextricably linked to the people element. For example, group size, a transparent composition of members, or community events directly impact the aspects above and should therefore be well thought out.

As mentioned earlier, members have different goals, and therefore members' individual goals can also influence the community's overall goals. People also shape the culture of the community through their values, attitudes, and behaviors. In addition, the geographic composition of people can influence the choice of infrastructure, such as venues. Finally, people's skills, experiences, and preferences can influence the selection and use of technologies such as communication tools or processes and procedures such as decision-making processes, resource management, or conflict resolution strategies.

5.3 Culture

The culture of a sharing community includes its members' norms, values, expectations, and behaviors. In addition, culture includes various factors such as member engagement, the culture of the organizations they belong to, trust, collaboration, and communication within the community. Initially, culture is mainly brought into the community from the outside and unconsciously, e.g., by the members and their organizations. Then, the culture must be guided by the agreed-upon goals and values and grow.

It is vital to align the culture to support the sharing community's particular goals best. The sooner this is done, the better. Once cultural structures are established, they are difficult to change. Important cultural aspects in sharing communities are, for example, understanding and dealing with mistakes, which directly impact sharing behavior and collaboration, as described in Section 4.

Different elements can be affected depending on the prevailing culture. For example, if a community strives for a culture of openness, trust, support, and learning, members might be more willing to share openly, work closely together, and support each other. This way, specific goals might be achieved more quickly and effectively, or processes and procedures might be improved. In contrast, a highly results-oriented culture might encourage the achievement of specific, measurable goals. In addition, a culture of mistrust influences people and forces the turnover of people or the formation of subgroups. Another example could be a sustainable culture leading to the usage of sustainable transportation infrastructure for community events. Finally, a reserved and conservative culture can further influence the selection or trial of new technologies.

5.4 Processes and Procedures

Processes and procedures contribute to the functionality and quality of collaboration by creating clear structures, guidelines, or policies for members. Defining roles, responsibilities, and common goals within the community can enable effective collaboration and communication. Establishing structures for regular meetings, calls, and in-person events is vital to promote trust, information sharing, and collaboration. Selecting and implementing the right technologies for sharing, communication, and collaboration is critical to ensure a smooth flow of information. In this context, it is essential to establish rules for sharing CTI, including the type of CTI, formats used, and standards.

The quality of shared CTI is a critical issue, and guidelines would help achieve a minimum level of quality by, for example, mandating certain contextual information. Transparent procedures for problem-solving and decision-making within the community are

also necessary to ensure an effective and productive work environment. Regulating membership in the sharing community ensures a diverse, competent, and engaged group. Onboarding and training processes for new members are important to integrate them into the community and familiarize them with existing processes and procedures. Finally, rules and solutions for member misconduct could be established and documented to maintain a positive work environment.

The sharing community can collaborate effectively, share valuable CTI, and achieve mutual goals and benefits by establishing and continuously improving these processes and procedures. These processes and procedures must be accessible and understood by all members of the sharing community to ensure their acceptance and implementation, which influences the people and culture in the community. In addition, defined policies impact infrastructure and technology by determining what infrastructure and technology should be used.

5.5 Infrastructure

Infrastructure refers to the resources and organizational structures that support the operation and functioning of a community. This includes physical and virtual resources, facilities, and services enabling members to meet, collaborate, and share information. Members of sharing communities meet regularly for various occasions, such as (informal) meetings or conferences. In this context, facilities such as restaurants or conference rooms, equipment, Internet connections, or functional communication systems are needed so that members can cooperate. In this context, wrongly chosen facilities, insufficient space, or missing technical equipment hinder cooperation. In addition, information security also plays a vital role in the communication channels used at venues, which should not be neglected. In the case of venues or conferences, additional personnel is also required to manage the conference on-site. In a broader sense, infrastructure can also include means of transportation necessary to get to meetings or conferences. However, it is important to point out that the infrastructure of a sharing community is mainly the technology the members use to communicate and share.

Face-to-face encounters and regular interactions are critical factors in building trust. Without this personal contact, it can be challenging to build trust between people, making it difficult for newcomers to join a community. This can affect elements like people, the culture of a community, and the achievement of goals.

5.6 Technology

The technology element refers to the tools, platforms, systems, and applications that enable and support information sharing, collaboration, and communication among members. Technology is critical to the success and functioning of the community as it provides the foundation for the most important tasks within a group.

As described in Section 4, technology use, standards, application, and implementation vary between groups. In addition, different sharing groups use different taxonomies or ontologies. To date, there is no one best practice or tool used by every community for CTI sharing, communication, and collaboration. Widespread standardization of technologies, standards, and formats among sharing communities would positively impact the totality of all groups and make members' daily work more effective and efficient, increasing the overall performance of sharing communities.

Most sharing communities rely on technology for operations. Therefore it is a fundamental basis and affects many other elements. Without a communication channel, people can not cooperate and communicate with each other. Moreover, cumbersome and poor tools can negatively impact morale and, thus, the people and culture in the community. Goals are also influenced by technology, as there are technologies that make communication and collaboration more effective and efficient, promoting goal achievement. Certain technologies, such as artificial intelligence, also impact processes and procedures by improving, automating, or accelerating specific tasks such as incident analysis.

5.7 External Factors

Sharing communities are embedded within an outer frame that includes a regulatory framework, financial or economic factors, and stakeholders. Those factors influence the organizational structures described in Section 4.2 and the community's functioning, objectives, and results.

The legal and regulatory framework for sharing communities refers to local, national, and international laws and regulations that affect information sharing, privacy, and security. These regulations include the European General Data Protection Regulation (GDPR), company-specific compliance rules, or NDAs. These make it difficult or even impossible for certain members to share CTI. This can be a barrier to success and achievement of goals within the community. In addition, the composition of members may be impacted by laws such as sanctions or geopolitical conditions that affect all elements and do not allow certain members to participate.

As different types of costs are incurred, financial and economic factors also play an essential role in the functioning of sharing communities. Examples of costs within a sharing community are costs for the maintenance of technology, software development, subscriptions for specific tools, insurance for risks through sharing, or costs for personnel and administrative tasks such as organizing meetings or events. The financial and economic factors influence the scope and depth of collaboration by impacting the available technologies and time resources of people. They improve or worsen the group's effectiveness, efficiency, and performance.

Another external factor influencing a sharing community is stakeholders such as constituencies, government agencies, investors, customers, and environmental groups. Another group of stakeholders is the support function within a sharing community. These individuals perform various tasks such as organizing events and meetings for sharing community members or writing protocols and completing paperwork. Therefore, these stakeholders influence the functioning of the system. In contrast, other stakeholders, such as the public, regulators, and other government agencies, benefit from increased security through the efforts of a sharing community without contributing much or anything.

6 DISCUSSION

In this section, we first discuss the organizational structures of sharing communities regarding RQ1. We then explore members'

goals and the benefits of sharing and participating in a sharing community regarding RQ2. Subsequently, we discuss the prevailing challenges in sharing communities, considering our analysis with STS theory (RQ3). Finally, we discuss the application of STS theory and potential threats to the validity of our results.

RQ1: Structures. The results of the interviews show a wide variety of organizational structures of sharing communities. They differ in terms of the types of groups, member profiles, number of members, maturity, and roles of members, and collaboration tools and practices. Knowing the different types and their advantages and disadvantages is important for achieving maximum benefit. In addition to the long-term open and closed groups, there are the temporary specific groups. For increasingly complex attacks, participation in several different sharing communities is often necessary for a successful defense. This requires members of a variety of different tools to communicate and share.

The lack of transparency in most communities results in an unclear membership base and roles, making it difficult for communities to find appropriate members and for members to find the right community. However, this matching accuracy is essential for effective and efficient collaboration and information sharing. In addition, the size and maturity of members significantly impact other factors of a sharing community, such as the scope and quality of exchanges or trust. The optimal size of a sharing community depends on the group's goals, priorities, and members, balancing outreach and trust.

RQ2: Goals & benefits. It could be shown by the experts that the members of sharing communities have different goals. However, open communication, as well as understanding the goals of other members, is crucial for the overall success of a sharing community, as it positively influences member interaction and collaboration. Similar goals can foster synergy and strengthen communities, whereas competing goals can slow down the overall effectiveness of the community. Accordingly, developing and aligning common goals in the community is a key success factor.

The benefits members see from sharing and participating in these communities show how important these groups are to cyber defense and strengthening overall cybersecurity worldwide. One interviewee underscores this by emphasizing that "sharing communities are super critical to the stability of the Internet today". The benefits can be categorized at the micro, meso, and macro levels, highlighting the broad mechanisms of influence and impact of sharing communities. In addition to the classic benefits of sharing, such as cost efficiency, expert access, and community building, sharing communities also provide other specific benefits, such as increased visibility of the threat landscape or additional context. However, when considering the benefits presented, it is important to consider that the extent to which members experience them depends on the type and size of the community. As shown by interviewees, these benefits are far more likely to be realized in smaller, trust communities where members know each other.

RQ3: Challenges. As we determined through the interviews, sharing communities and their members have to face a wide variety of challenges. These cannot be minimized to purely technical problems. One expert also underlined this, emphasizing that "if it were all this technical and engineering stuff, then we would have solved much of this long ago. Unfortunately, it is still just people's problems". Since a significant part of the work in sharing communities takes place through the collaboration of people, the social and interpersonal aspects within these groups play a fundamental role in mastering the challenge and the overall success of the communities. Moreover, the causes of the challenge cannot simply be attributed to individual factors; instead, they are multifactorial reasons that contribute to the emergence of many of the challenges we have outlined.

It is necessary to conduct a holistic investigation to understand the causes of the challenges and develop practical solutions. For this purpose, using the STS theory and supporting the interviews' findings is valuable, including the investigation's social, technical elements, and external factors. This helps to understand complex interrelationships better and is essential to achieve the maximum success of changes.

Trust, which was mentioned as a key factor, is directly related to challenges such as the lack of sharing or the formation of subgroups. Transparent organizational structures and objectives are essential for trust within a sharing community. Since trust is built primarily on an interpersonal level, members' commitment is also essential. Members must be aware of the benefits of sharing communities to make the necessary effort to build and maintain a trust network. Promoting open and transparent communication between members and open feedback, error, and tolerance culture also strengthens trust. For example, this could be supported through regular meetings, community events, joint events, or even joint projects. Those factors can also build common ground, mutual understanding, and uniform values, contributing to better bonding and belonging. In addition, clear guidelines and a secure technical and legal framework are important to ensure members have a trustworthy space with the highest possible level of protection.

Guidelines and standards could also help mitigate other challenges, such as the lack of quality and sharing of CTI. For example, those could define the extent to which feedback and context are provided or what quality attributes should be considered in the shared information. This should be combined with audience-specific education and training, both at the outset and on an ongoing basis, to increase members' knowledge of creating and assessing the quality of CTI. This can increase member maturity, which is an additional adjusting screw for the quality and quantity of information exchange. In addition to these preventive measures, additional technical solutions such as sophisticated feedback mechanisms or quality management monitoring systems could address CTI quality challenges and thus lead to improved information sharing. In particular, extrinsically motivated members can be spurred on to higher exchange activity or feedback via incentives.

The existing conditions in sharing communities, such as the high level of complexity and information overload, time pressure in incident situations, rapid change, and self-responsibility, are associated with an increased risk of mental stress and illness for members. Considering the challenges with recruiting new members and the long-term personal trust-building and contact maintenance, the relevance of this problem is further increased. The feeling of being unable to afford extended time off or downtime also leads to a lack of rest and working while ill, which increases the error rate and reduces the quality of shared information and performance. This, in turn, directly impacts challenges such as lack of feedback

or context. The lack of quality leads to certain groups becoming less relevant to members, and these groups begin to atrophy, and a lack of sharing occurs. This leads to fluctuation in the group, and members start to form new subgroups.

These challenges can be prevented or minimized by an open, supportive atmosphere with a transparent, error-friendly, and values-based culture and collaboration. Members should feel comfortable in the community, trust each other, and be able to ask and receive each other's questions, feedback, and help. Many of these supportive factors for healthy, resilient structures and relationships can be copied from other successful organizations with the help of STS. The earlier, ideally, when a sharing group is founded, these factors are considered and actively shaped, the fewer hurdles and challenges will arise. This forward-looking planning can make sharing communities sustainable, stable, and successful even during diverse social changes, normative shifts, or crises.

Analysis with STS. Applying STS theory gave us a deeper understanding that sharing communities are complex socio-technical systems. Viewing these structures through the STS framework allowed us to analyze them from micro to macro level by examining the individual elements, their interactions, and finally, the whole system's function. This helped us gain a holistic view of sharing communities' organizational structures and challenges.

STS theory allowed us to understand that social and technical factors in sharing communities are closely interrelated and significantly affect the structure and functioning of communities. For example, technical changes, such as a new sharing tool, can impact organizational structures by requiring new working methods or communication patterns. At the same time, social changes, such as membership composition, can affect how technologies are used in the community.

Furthermore, STS helped us better understand that challenges might have multiple technical and social roots. Social challenges such as trust can influence what kind of information is shared. Conversely, poor technology can affect members and how they collaborate. By applying STS theory, we could see that these challenges cannot be viewed in isolation but rather in the context of social and technical factors influencing each other.

In this work, we were able to show how the individual elements and their interrelationships influence sharing communities through the STS framework and how important this consideration is for the foundation and existing communities. As a result, the cooperation and the information exchange of sharing communities can be sustainably optimized.

Threat-to-validity. Finally, we want to acknowledge that our unintentional all-male sample may narrow certain perspectives and the generalizability of our findings. Our recruitment strategy was gender-neutral. Based on the criteria of our desired target sample, both women and men were contacted. Our sample should be viewed as a reflection of the gender imbalance in the industry, which is a general systematic problem. This was also underscored by the interviewees' desire for more diversity and highlighted an industry-wide concern. Furthermore, we want to emphasize that our work does not aim not for broad generalizability but a deep understanding of the phenomena under study. Generalizability, as understood in quantitative research, is not the primary goal of qualitative research. Instead, we aim for a detailed, contextual understanding.

Future research. Future research efforts should further deepen the understanding of the holistic view of sharing communities to improve CTI exchange and collaboration among members. One possible approach would be case studies in which the STS framework is applied to concrete sharing communities in practice. This could provide more detailed insights into how they work. In addition, the individual challenges we have identified should be analyzed in more depth using the STS framework, and best practices and concrete recommendations for action should be developed on this basis. Additionally, future research could work to develop metrics and evaluation systems to measure the effectiveness, performance, and impact of sharing communities to understand their impact on cyber defense better. By considering these specific research directions, future work can help strengthen collaboration and information sharing within sharing communities, thereby optimizing their contribution to cyber defense.

7 CONCLUSION

In this study, we conducted expert interviews to learn more about the organizational structures and challenges of sharing communities in practice. In addition, we used STS theory to deepen the insights from the interviews and better understand the interrelationships between social and technical elements of sharing communities. This additional analysis helped us contextualize our findings and better understand their interrelationship. Furthermore, it allowed us to understand better the influence of social and technical elements and their interaction on sharing communities.

Our work presents a comprehensive and holistic approach to better understanding and improving sharing communities. We address the positive aspects, such as the goals and benefits (the good). We also highlight the prevalent problems and challenges (the bad). Our findings show that sharing communities are complex systems where individual social factors such as people or culture are as important as technical elements. This must be considered when addressing the challenges and problems of sharing communities in practice. Finally, holistic solutions that consider the interrelationships between technical and social elements need to be developed, which will not be trivial (the ugly). This is important to improve the effectiveness, efficiency, and performance of sharing communities over the long term. Sharing communities and their many dedicated members are crucial assets for cybersecurity.

ACKNOWLEDGMENTS

We express our sincere gratitude to Alexandra Paulus, who assisted us in creating and evaluating the questionnaire. Moreover, we would also like to thank the experts who gave their valuable time and expertise to help us conduct this study. The expertise and experience of Alexandra and the experts were indispensable to the success of this work. Finally, we would like to thank all the dedicated members of sharing communities who often volunteer and participate in these communities for charitable and community interests. This often involves a lot of work and commitment, but it helps create a positive and supportive environment for all of us. This work was supported by the German Federal Ministry of Education and Research (BMBF) as part of the DEVISE project.

REFERENCES

[1] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. 2020. A different cup of TI? The added value of commercial threat intelligence. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, USA, 433–450. https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman

[2] Xander Bouwman, Victor Le Pochat, Pawel Foremski, Tom Van Goethem, Carlos H. Ganan, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Wouter Joosen, and Michel van Eeten. 2022. Helping hands: Measuring the impact of a large threat intelligence sharing community. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 1149–1165. https://www.usenix.org/conference/usenixsecurity22/presentation/bouwman

[3] G. A. Bowen. 2008. Naturalistic inquiry and the saturation concept: a research note. *Qualitative Research* 8, 1 (2008), 137–152. https://doi.org/10.1177/1468794107085301

[4] Rose Challenger and Chris W. Clegg. 2011. Crowd disasters: a socio-technical systems perspective. *Contemporary Social Science* 6, 3 (2011), 343–360. https://doi.org/10.1080/21582041.2011.619862

[5] Albert Cherns. 1976. The principles of sociotechnical design. *Human relations* 29, 8 (1976), 783–792.

[6] Thomas Y Choi, Kevin J Dooley, and Manus Rungtusanatham. 2001. Supply networks and complex adaptive systems: control versus emergence. *Journal of Operations Management* 19, 3 (2001), 351–366. https://doi.org/10.1016/S0272-6963(00)00068-1

[7] Chris W. Clegg, Mark A. Robinson, Matthew C. Davis, Lucy E. Bolton, Rebecca L. Pieniazek, and Alison McKay. 2017. Applying organizational psychology as a design science: A method for predicting malfunctions in socio-technical systems (PreMiSTS). *Design Science* 3 (2017), e6. https://doi.org/10.1017/dsj.2017.4

[8] Central University Research Ethics Committee (CUREC). 2020. *Elite and Expert Interviewing: Best Practice Guidance 03_Version 4.0.* University of Oxford.

[9] Matthew C. Davis, Rose Challenger, Dharshana N.W. Jayewardene, and Chris W. Clegg. 2014. Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics* 45, 2, Part A (2014), 171–180. https://doi.org/10.1016/j.apergo.2013.02.009 Advances in Socio-Technical Systems Understanding and Design: A Festschrift in Honour of K.D. Eason.

[10] FIRST. 2023. FIRST History. https://www.first.org/about/history

[11] Cornelia Helfferich. 2011. *Die Qualität qualitativer Daten (The quality of qualitative data)*. Vol. 4. Springer, Germany.

[12] Software Engineering Institute. 2023. The CERT Division | Software Engineering Institute. https://www.sei.cmu.edu/about/divisions/cert/index.cfm

[13] Neil Johnson. 2009. *Simply complexity: A clear guide to complexity theory.* Simon and Schuster, England.

[14] Thomas Kinsella. 2022. Why Your Security Analysts Are Leaving and What You Can Do to Retain Them. https://www.first.org/resources/papers/cti22-berlin/Thomas-Kinsella.pdf

[15] Nina A. Kollars and Andrew Sellers. 2016. Trust and information sharing: ISACs and U.S. Policy. *Journal of Cyber Policy* 1, 2 (2016), 265–277. https://doi.org/10.1080/23738871.2016.1229804 arXiv:https://doi.org/10.1080/23738871.2016.1229804

[16] Jan Kruse and Christian Schmieder. 2014. *Qualitative interviewforschung (Qualitative interview research).* Beltz Juventa, Germany.

[17] Udo Kuckartz. 2007. Einführung in die computergestützte Analyse qualitativer Daten (Introduction to computer-assisted analysis of qualitative data).

[18] Udo Kuckartz. 2018. Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4. Aufl. (Qualitative content analysis. Methods, Practice, Computer Support, 4th ed.) Beltz Juventa.

[19] George Lawton. 2009. On the Trail of the Conficker Worm. *Computer* 42, 6 (2009), 19–22. https://doi.org/10.1109/MC.2009.198

[20] HJ Leavitt and JG March. 1965. Applied Organisational Change in industry: Structural, Technological and Humanistic Approaches, Carnegie Institute of Technology. *Graduate School of Industrial Administration* 1st edition, 1 (1965), 1144–1170.

[21] Adobe Systems Software Ireland Limited. 2022. Audio and video editing software, Version 22.5 (Build 62). https://www.adobe.com/

[22] Bryan Marshall, Peter Cardon, Amit Poddar, and Renee Fontenot. 2013. Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. *Journal of Computer Information Systems* 54, 1 (2013), 11–22. https://doi.org/10.1080/08874417.2013.11645667

[23] MISP. 2023. MISP Open Source Threat Intelligence Platform; Open Standards For Threat Information Sharing. https://www.misp-project.org/

[24] Hilarie Orman. 2003. The Morris worm: A fifteen-year perspective. *IEEE Security & Privacy* 1, 5 (2003), 35–43.

[25] Hideyuki Tanaka, Kanta Matsuura, and Osamu Sudoh. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy* 24, 1 (2005), 37–59.

[26] Thomas D Wagner, Khaled Mahbub, Esther Palomar, and Ali E Abdallah. 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security* 87 (2019), 101589.

[27] Adam Zibak and Andrew Simpson. 2018. Can We Evaluate the Impact of Cyber Security Information Sharing? *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (2018), 1–2. https://doi.org/10.1109/cybersa.2018.8551462

[28] Adam Zibak and Andrew Simpson. 2019. Cyber Threat Information Sharing. *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), 1–9. https://doi.org/10.1145/3339252.3340528

[29] Adam Zibak and Andrew Simpson. 2019. Towards Better Understanding of Cyber Security Information Sharing. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (2019), 1–8. https://doi.org/10.1109/cybersa.2019.8899697

[30] Inc. Zoom Video Communications. 2022. Video conferencing software, Version 5.10.6 (5889). http://zoom.us/

A DEMOGRAPHICS

No.	Gender	Exp.	Jobtitle
1	Male	20 +	Vice President of CTI
2	Male	10	Chief Technical Officer
3	Male	20 +	Head of CERT
4	Male	20 +	Chief Executive Officer
5	Male	14	Director Cybersecurity TI
6	Male	7	Head of Defense
7	Male	20	Manager of Outreach
8	Male	35	Lead of Incident Responders
9	Male	20	Cyber Security Consultant
10	Male	15	Chief Regulatory Advisor
11	Male	14	Chief Cybersecurity Advisor
12	Male	10	Senior Advisor
13	Male	18	Expert Advisor
14	Male	20 +	Principal Analyst
15	Male	10	CTI Analyst
16	Male	10 +	Security Analyst
17	Male	7	Security Analyst
18	Male	10	Principal Specialist
19	Male	16	Senior Internet Security Specialist
20	Male	15 +	CERT Specialist
21	Male	6	CTI Specialist
22	Male	7	Senior Researcher CSIRT
23	Male	20 +	Threat Hunter
24	Male	6	Key Expert for TI
25	Male	10 +	Chief Architect

B INTERVIEW MATERIAL

Showed Definitions:

Cyber Threat Intelligence: Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Sharing Community: A sharing community is an association of two or more participants sharing CTI with other participants.

Questions related to the interviewee:

(1) In which field(s) do you work?
(2) How is your position called?
(3) How long have you been working in this position?
(4) In which context do you work with CTI?
(5) How long have you been working with CTI?
(6) Which goals do you have through CTI-sharing?

Questions related to sharing communities:

(1) What do you think are the different roles in a sharing community?
(2) How do you integrate yourself and your organization into a sharing community?
(3) Who, to your knowledge, are participants in sharing communities?
(4) Which participants do you think need to be part of a sharing community to achieve your goals (by participating in a sharing community)?
(5) Does a sharing community scale?
(6) What kind of CTI, shared in a sharing community, are relevant for you?
(7) Do you use platforms for CTI-sharing?
   - If yes, which platforms do you use?
   - If not, what do you use instead to exchange, obtain or offer CTI?
(8) What added value do you or your organization expect from a sharing community?

Questions related to CTI & quality management:

- Not applicable for this work.

Questions related to innovations and challenges:

(1) What innovations or actions would lead to an improvement of CTI-sharing?
(2) Where do you personally see challenges in the exchange of CTI?

Closing questions:

(1) Can you think of anything else you would like to tell us?
(2) Can you recommend some interview partners?

C CATEGORIES ACCORDING TO KUCKARTZ