Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study

Vilja Steffensen and Vahiny Gnanasekaran

Norwegian University of Science and Technology (NTNU), Trondheim, Norway
vahiny.gnanasekaran@ntnu.no

Abstract. The number of cyber incidents is steadily increasing in all sectors. Not all sectors have access to cybersecurity personnel with domain-specific knowledge, which further motivates the need for a Computer Security Incident Response Team (CSIRT). However, for a CSIRT to function as intended, effective digital communication should be at the forefront. This paper uses a case from the Norwegian municipality sector to explore the communication practices between the CSIRT and its members. Ten semi-structured interviews with eleven participants representing the CSIRT and the municipalities were conducted. The findings include the most used communication channels and the members' perceptions of information sharing. Key factors limiting information sharing are the size of the municipality and access to critical resources, geographical location, and the lack of personal networks. Future work should investigate the generalizability of the findings in other sectors and countries.

Keywords: CSIRT · Critical infrastructure · Communication practices · Municipality.

1 Introduction

The cybersecurity threat landscape continues to worsen with the larger part of the Western world being at war. As a result of the ongoing geopolitical crisis, the European Union Agency for Cybersecurity (ENISA) is experiencing a growing number of cyber incidents and threat actors targeting public and private organizations [4]. This demanding threat landscape increases the need for a Computer Security Incident Response Team (CSIRT).

In Norway, most businesses rely on their sector-specific CSIRT to support their cybersecurity efforts, as they may lack the expertise or resources to operate their own. The Norwegian municipalities are responsible for several sectors and needed to communicate with CSIRTs from multiple sectors. This has reportedly hindered incident response, as the coordination between the different SRMs has not been satisfactory [18].

The communication issue has also gained more attention in the literature the recent years [7,10]. Previous work [10,12,23] identified the importance of information sharing, and trust before and during incident response. However, many national Computer Emergency Response Teams (CERT)s are still using manual processes to distribute and communicate threat information to their members [11]. As a result of the increasing number of cyber threats targeting public administration in Europe, in addition to serious concern among Norwegian municipalities about their cyber resilience, it becomes more critical to study information sharing between CERTs/CSIRTs. Information sharing in this context denotes the exchange of information about vulnerabilities and other threats relating to cybersecurity in the municipalities.

Although trusted personal networks are recognized as a crucial factor in enhancing information sharing [8,10,17], how information sharing is established in a Norwegian context is less discussed. This paper aims to study the digital communication practices between a CSIRT and its members, by applying the recently established CSIRT for the Norwegian health and municipality sector (norw. "Helse- og KommuneCERT", henceforth Health- and MunicipalityCERT) as a case. Based on insights from ten CSIRT representatives and municipalities, the study presents how information is shared between the members and the CSIRT and the members' feedback on the current practices. More specifically, the research questions are:

- **RQ1:** What digital communication channels are used between a sector-specific CSIRT and its members?
- **RQ2:** What factors limit information sharing between a sector-specific CSIRT and its members?

This study is relevant for cybersecurity professionals working in public-administrative organizations, and security researchers that seek to understand CSIRT communication practices. Grasping the means of intra- and inter-member communication contributes to identifying unknown communication opportunities during incident response.

2 Background and Related Work

This section briefly overviews the related work, selected frameworks, and legislations affecting the CSIRTs, both from a European and Norwegian perspective.

2.1 Computer Security Incident Response Team (CSIRT) Services

Cybersecurity teams are uniquely organized based on what services they provide, their focus, and their constituency. Even teams that focus on incident handling like CSIRTs differ from each other. Table 1 describes similarities and differences between some commonly known cybersecurity teams. The Handbook for Computer Security Incident Response Teams (CSIRTs) from Carnegie Mellon University (CMU) presents a framework explaining the CSIRT organization and their common services and responsibilities, information sharing, and relationships with other cybersecurity teams [25]. According to the framework, CSIRT must provide at least one of the following incident handling services to be considered a CSIRT:

- **Incident analysis** involves the examination of evidence and identifying the scope of the incident. The handbook further explains two sub-services: forensic evidence collection and tracking or tracing.
- **Incident response on site** necessitates physical assistance at the incident's location to help the affected constituent recover.
- **Incident response support** indicates assistance via e-mail, phone, or similar means of communication.
- **Incident response coordination** includes notifying parties potentially involved with the incident, coordinating with law enforcement, and the response efforts among the relevant parties.

The European Union Agency for Cybersecurity (ENISA) is responsible for securing Europe by coordinating with national CSIRTs and other important stakeholders. When they describe the tasks of a CSIRT compared to a SOC, the most important distinction is the CSIRTs focus on coordination and communication with different stakeholders and constituencies [3]. Both ENISA and CMU regard CSIRTs to have the same capabilities as a CERT. This paper will henceforward address CERTs as CSIRTs to avoid confusion.

2.2 Related Work

The literature reports of similar qualitative studies conducted in other countries, such as Germany [17], and Netherlands [10]. In Germany, after initial reporting, the CSIRTs apply a ticketing system (e.g., OTRS) to collect evidence for cyber incident response. The finding is also further supported by Kassim et al. [11], where they use an online survey (N=19) to explore reporting tools for national CSIRTs. The results indicated a lack of a standardized reporting tool. However, the sample is too small to make generalized assumptions. Still, it provides an overview of other practices in countries not included in other works (e.g., Sri Lanka, and Bangladesh). Both studies addressed an increased usage of time-consuming, manual procedures, due to the lack of a shared platform. Van der Kleij et al. [10] highlight the issue from the cognitive sciences, and emphasize the role of communication. They further address the trust needed between the CSIRT and their members, claiming that members are reluctant to share incident information fearing a reputational loss. The members would rather face the threats alone without involving the CSIRT community.

Trust is addressed as a critical factor in sharing incident data with others [23]. Riebe et al. [17] emphasized the relevance of personal bonds to both technicians and other non-technical personnel. Another paper researching how anonymity and trust influence cybersecurity collaboration, reports that initial face-to-face interaction significantly improves information sharing [12]. The trust between a CSIRT and its constituency was already recognized as an important aspect of promoting information sharing by CMU [25]. It must be earned and nurtured to

Table 1. Teams in the security incident response field.

Term	Explanation
Computer Emergency Response Team (CERT)	CERTs carry the same responsibilities and tasks as a CSIRT. The term is often used interchangeably with CSIRT [21].
Incident Response Team (IRT)	IRT was commonly used to describe security teams, but as the need for better cooperation between those teams became apparent, most current CSIRTs are not solely focused on the incident response. Regardless, many still use the term 'IRT' today, and the two terms are used interchangeably.
Security Operations Center (SOC)	The core activities of CSIRTs are reactive services, while SOCs focus on proactive services, although SOCs are usually tasked with handling security incidents discovered through monitoring. While the extent of CSIRTs often encompasses sectors or countries, SOCs are usually positioned in a company and provide in-house or outsourced services [3].
Information Sharing and Analysis Center (ISAC)	The focus of ISACs lies in facilitating information sharing. As this has become an important focus area for CSIRTs as well, they have similar constituencies, e.g. by being sector-specific [2]. Some work prefer the establishment of an ISAC than a CSIRT as it is recognized as being better at raising awareness of cybersecurity in immature sectors and improving communication [8,20].
SRM	Sector-specific CSIRT (norw. "sektorvise responsmiljø") follow the Norwegian framework for managing cyber incidents and are in the Norwegian context synonyms with sector-specific CSIRTs.

get the constituency's support and for the CSIRT to operate effectively. They also emphasize the importance of clarifying the responsibilities of different CSIRTs that may share an overlapping constituency. If those CSIRTs do not coordinate well enough, duplicated efforts may antagonize all parties involved. This has also been one of the reasons not to establish a construction-specific CSIRT in Norway, since it can lead to more confusion in an immature sector [20]. In the context of the municipality sector, this is highly relevant, because it involves many different stakeholders in different sectors.

Findings from related work [8,10,12,17] identify the importance of trust to promote information sharing in the context of cybersecurity incident handling. Building personal networks is important to achieve this. For instance, a report identified that information sharing in the health sector occurs mostly through established networks, coincidences, and enthusiasts. Hence, they recommend the establishment of an SRM dedicated to the municipality sector, as an ISAC at its core [15]. In a European context, ENISA further addresses trust as the most important element to improve collaboration [2]. The best tool to achieve this is personal relationships, but they do mention other mechanisms as well, e.g. sharing useful information in real-time, and the use of Traffic Light Protocol

(TLP). However, it is also recognized that personal networks are a challenge to maintain, especially as people change careers. Additionally, they acknowledge that laws can enforce incident reporting, but not enhance trust or decrease risks. Although this report focuses on ISACs, it is also applicable to CSIRTs that share these information-sharing responsibilities [2].

2.3 Relevant Frameworks and Legislations

This section introduces one Norwegian and one European framework, and the NIS2 directive. Other relevant framework exists (e.g., NIST), but these were selected due to their geographical relevance and novelty. The Norwegian National Security Authority (NSM) introduced the *framework for managing cyber incidents* to clarify the responsibility to maintain intra- and intersectoral information sharing and how to be better equipped in responding to critical cyber incidents across sectors. The different departments are responsible for identifying their SRM [16]. These are responsible for communicating with the members of the national CSIRT part of NSM, and with other SRMs.

ENISA supports the CSIRT Services Framework, which is hosted and regularly improved by the FIRST [3]. This framework divides the activities of CSIRTs into five main service areas: information security incident management, vulnerability management, situational awareness, knowledge transfer, and information security event management. FIRST was established to facilitate better coordination and communication across the increasingly many security groups that were formed at the time.

The NIS2 Directive (EU) replaces the current NIS1 Directive currently in effect [5]. The NIS Directive aims to enhance the cybersecurity level in the EU through regulation. However, the implementation is too inconsistent between the different EU Member States. For instance, an organization can be affected by legislation in one EU country but not other countries. The directive introduces a clarification of CSIRTs' requirements, both in terms of information sharing and services, and aims to enhance cooperation with the CSIRTs through regulation. This includes reporting obligations, where essential or important entities must, e.g., notify their CSIRT in case of significant incidents within 24 hours. In case of non-compliance, the new directive introduces worse repercussions, including a maximum fine of EUR 10,000,000 for essential entities. The directive introduces additional responsibilities for *competent authorities* and *single points of contact* [5]. The NIS2 Directive presents several new responsibilities delegated to ENISA. These include facilitating a European vulnerability register, and being the secretariat of the European Cyber Crises Liaison Organisation Network (CyCLONe), a cooperation network between the different national authorities to manage large-scale cyber incidents in the EU [1]. Its objective is to exchange information and build trust between members.

NIS2 Directive will greatly affect Norwegian countries and municipalities [14]. However, the NIS1 Directive is currently not legislated. The Norwegian Digital Security Act implementing NIS1 is expected to come into force in late 2024, and the government is working on updating the Norwegian Digital Security Act to the NIS2 directive. Still, Norwegian businesses operating in Europe are expected to comply with NIS2 legislated this year. Concerns are raised about the slow pace Norway implements the EU regulations. However, it is widely recognized that NSM's inherently fulfill the responsibilities of a competent authority [13].

3 Methodology

This section presents the selected research methodology, approach, and justification for the research methodology. Since incident handling protocols are often considered sensitive information, the most appropriate research method is a qualitative method approach. Researching social and behavioral phenomena identified in cybersecurity often requires qualitative methods to gain deeper insights than what quantitative research methods can do [6]. Semi-structured interviews were opted for, which is the most common method used in both organizational and personal cybersecurity research [6]. Semi-structured interviews are suitable whenever the research intends to study opinions, attitudes, and experiences [24]. The semi-structured nature allowed for comparing the participants' insights, while still letting them include crucial information to improve the interview guide. The participants have valuable insights that are difficult to find publicly available information on due to the inherent secrecy associated with incident handling.

The data collection followed all relevant regulations and practices regarding ethical approval, GDPR compliance, and informed consent, and occurred in the first half of 2024. The national research data collection tool *Nettskjema* was used for the pre-questionnaires and informed consent forms. Since they were semi-structured, the interviews were individually adapted to fit each interviewee. A summary of the interview guide is provided, with a distinction between the municipality CSIRT and the members, since they were structured differently:

- Usage of digital communication channels with the CSIRT/members.
- Their perception of the information sharing between CSIRT/members.
- Norwegian Digital Security Act preparedness.
- CSIRT/member expectations to the information sharing between CSIRT/members.
- Challenges concerning IT operations.

Trust between interviewer and interviewee is an important factor to enhance the quality of the semi-structured interviews [24]. Before the CSIRT interviews, a physical meeting was organized to explain the study's motivation. Similarly, a meeting was also conducted with the first representative from a municipality. The meetings further adapted the interview guides to the CERT and the members. Still, an interviewer bias might be present, due to the understanding of the questions might be different for each participant [9]. The bias was attempted mitigated by sending the questions in advance to let the interviewees provide feedback and questions. Since the study aims to understand information sharing between CSIRTs and members, some might not include confidential information.

In total, there were ten interviews, with eleven participants. The first two were CSIRT representatives, while the rest represented members or partners of municipality CSIRT. The last interview was conducted with two participants from the same municipality. The interviews lasted between 35 and 60 minutes. The first three were conducted physically, and the rest on Teams. For the audio recording, the national research data collection tool was applied, which automatically transcribes the interviews using Whisper on their infrastructure. Each participant was assigned an ID to ensure anonymity in the transcripts. The links between the participants and their IDs were managed in an Excel file. After summarizing the findings, the quotations were controlled by the participants to clear up any misunderstandings, and to ensure that every participant was satisfied with the anonymization [24].

Recruitment Communication practices in this context rely on gathering insights from cybersecurity professionals at the CSIRTs, and its members. An opinion piece was published to recruit the most fitting participants. The text drew the attention of Health and MuncipalityCERT, where two participated. Three representing the members were recruited through the authors' network. During one of the interviews, a forum for aiding municipalities in cybersecurity was suggested for recruiting. The forum was contacted through social media to participate in the interview study, resulting in three additional participants. The remaining three were recruited through e-mail from other interviewees. Recruiting municipalities to join the interview study was challenging, particularly for the smaller municipalities. This required the use of personal networks and posts online to recruit since participants are more willing to interview when they are suggested by acquaintances or other colleagues. Hence, a sampling bias could be present in the interview study [19]. However, since the cybersecurity field is not large in Norway, information power, i.e. the amount of information gathered from each interview, could be considered more important to obtain than the sampling approach [6].

Data Analysis After all the interviews had been properly transcribed and anonymized, they were coded using NVivo. The objective was to generate *empirically-close* codes, meaning that the codes are not derived from preconceived ideas, but from the empirical material itself [24]. After coding the first two interviews, similar codes were grouped, and this was later done in parallel with coding the rest of the interviews. To ensure objective patterns, a calibration session with two other researchers was conducted. After coding all interviews, the groups were renamed to avoid the same coding categories. Table 2 show the coding categories structured into three tiers.

Sample Description An overview of the interview sample is provided in Table 3. CSIRT participants are labeled with CSIRT in their IDs, while members are labeled with MEMB. Some participants consider themselves as partners of

Table 2. A description of the top-level coding scheme in NVivo is provided with an example in each group.

Name	# Codes	Description	Example
Sample	2	Contains codes describing the participants' work experience and their description of a typical workday.	*"Work experience"* and *"Typical workday"*
The actors and communication channels in the sector	192	Contains codes describing the actors, communication channels, and information sharing as depicted in Figure 1.	*"Participates in webinars when friends will give a presentation"*
Regulation and challenges	199	Contains codes describing the participants' perspectives on NIS, supervisory authorities, and challenges of managing IT security in municipalities.	*"Health- and MuncipalityCERT believes that the culture of openness between cybersecurity teams could be improved"*
CSIRT expectations	178	Contains codes describing the participants' expectations of an SRM and the new assignment, and the members' opinion of the services provided by Health- and MuncipalityCERT.	*"Health- and MuncipalityCERT should learn a bit about onboarding or follow-up"*

Health- and MuncipalityCERT rather than members, but since they have all provided their perspectives on their communication practices with their CSIRT, they are referred to as members. The municipalities are anonymized to limit disclosing the participants, but the population provides information about the size. The population of the municipalities that consist of the IKS or are members are added together. For instance, IKS A consists of five municipalities, while IKS B has 13 municipalities that are currently or about to become members. A generalized job description is provided, due to the different sizes of IT departments at each municipality, the organizational structure and responsibility level might be different. Hence, 'IT professional' indicates a lower managerial position than 'IT officer'. The years of experience includes only the number of experience in their current position. Low indicates 1-5 years, medium indicates 6-9 years, and high indicates 10-15 years.

4 Case: The Norwegian Municipality CSIRT

This section provides a brief introduction to the CERT responsible for the health and municipality sector in Norway. Health- and MuncipalityCERT is the newly assigned CSIRT for the Norwegian municipalities and encompasses the health and municipality sectors. They provide a wide range of services but handle cyber

Table 3. Interview Sample Overview.

ID	Stakeholder	Title	Years	Population
CSIRT_11	Health- and MuncipalityCERT	IT-officer	High	-
CSIRT_12	Health- and MuncipalityCERT	IT-officer	Medium	-
MEMB_13	Municipality A	IT-professional	Medium	210 000
MEMB_14	IKS A	IT-professional	High	35 000
MEMB_15	Municipality B	IT-professional	Low	30 000
MEMB_16	IKS B	IT-officer	Medium	220 000
MEMB_17	Municipality C	IT-officer	Low	15 000
MEMB_18	Municipality D	IT-professional	Medium	710 000
MEMB_19	Municipality E	IT-officer	High	30 000
MEMB_20	Municipality D	IT-officer	Low	710 000
MEMB_21	Municipality D	IT-officer	Low	710 000

incidents by assisting their constituency with incident response and coordination, consisting of both reactive and proactive services.

Norsk Helsenett had previously established the CSIRT for the health sectors, making it one of the first Norwegian CSIRTs. They offer their members services through the program called NBP, including e.g. assessment of vulnerabilities and facilitating a sensor platform. Because of their focus on the health sector, they have a longstanding relationship with the municipalities. Hence, Norsk Helsenett was appointed the task of including a municipality CSIRT within their existing CSIRT. Today all municipalities, with very few exceptions, are members of Health- and MuncipalityCERT.

4.1 Stakeholders

The different stakeholders collaborating with Health- and MuncipalityCERT are represented in Figure 1 through the blue bubbles and rectangles, with Health- and MuncipalityCERT in the middle. The light blue figures represent the municipalities and their different perspectives, while dark blue represents the partners of Health- and MuncipalityCERT. The rectangles depicts CSIRT-like organizations, whereas the bubbles are the non-CSIRTs.

- **KommuneCSIRT** was the former CSIRT for the municipality sector. Several interviewees were familiar with the organization since some municipalities were members. However, after Norsk Helsenett was assigned the establishment of KommuneCERT, KommuneCSIRT was shut down. MEMB_17 expressed losing a critical advantage: *"We had something differently in KommuneCSIRT. [...] It was a bit easier since they were in Lillehammer [...], so you felt a bit more local affiliation."* The lost communication paths are represented in Figure 1 by the red crosses.
- **Oslo Municipality CSIRT.** Due to the size, Oslo municipality is mentioned separately since it deviates from the normal communication practices.

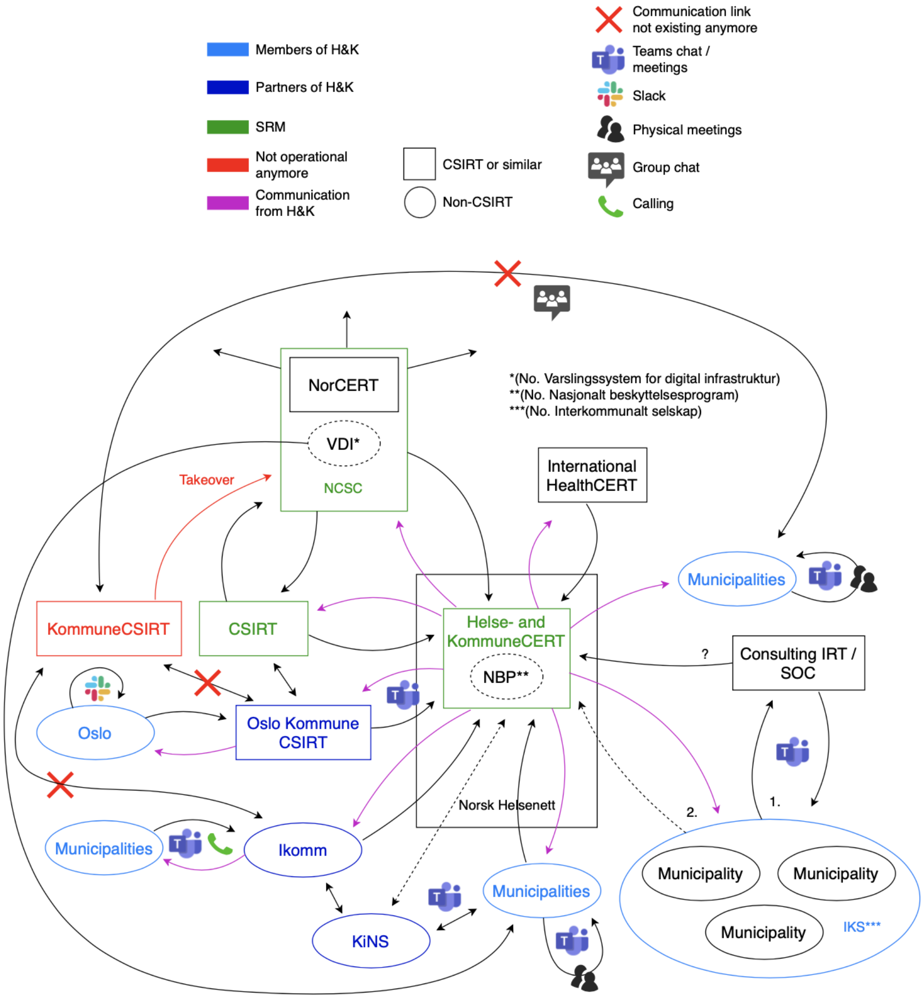

Fig. 1. Communication between members and the municipality CSIRT. IKS communicates through its external IRT provider, hence the numbering of the outgoing communication. Dotted lines denote a limited information sharing. In the case where information sharing has not been described any differently between two actors, a double-headed arrow is used.

It is the only municipality that has its own CSIRT, making them more independent than others. Oslo Municipality CSIRT is responsible for communicating with Health- and MuncipalityCERT on behalf of the municipality, but the CSIRT employees rarely communicate directly with Health- and MuncipalityCERT. Their services are similar to Health- and MuncipalityCERT, but targeted towards the internal, municipal departments.

- **Ikomm.** Small municipalities in Eastern Norway created Ikomm as a response to limited IT resources in each municipality. 13 municipalities are a member and owners of Ikomm, and mainly communicate through Ikomm. The company is a partner of Health- and MuncipalityCERT. Ikomm differs from IKS by being a privately-owned company with other costumers as well.
- **Consulting IRT and SOC.** Other members purchase security services from external companies (e.g., Ikomm). MEMB_14' municipality chose this approach since the external company is located near the municipality. Some security companies are approved by the national authorities but are not necessarily a partner with the CSIRT. Hence, it is unclear if they communicate with Health- and MuncipalityCERT.
- **Inter-municipality companies (IKS).** Similar to Ikomm, IKS was establish inter-municipality companies to simplify the IT operations of the neighboring municipalities. In particular, smaller municipalities which may find it difficult to employ people with the right expertise are a part of such communities.
- **KiNS.** A forum hosting different seminars about IT security and privacy for municipalities. Several participants were familiar with the organization, and some actively contributed to the network. The purpose is to establish a network to ask for support, especially for the workers who are solely responsible for the IT and/or security operations: *"KiNS, at least when I was in that position, played a very central role. We could call the larger municipalities. Bærum has been very active in KiNS for many years. You could call [someone] in Bærum and ask, 'What does this mean?"'* (**MEMB_16**).

4.2 Communication Channels

Figure 1 shows the relevant actors and their preferred means of communication. It provides an overview of the interviewees' perception of the information sharing between municipalities and CSIRTs (both the national CSIRT and the sector-specific CSIRT are shown), and which communication channels are being used. In general, the participants are satisfied with the availability of the CSIRT. At least two individuals at each member are responsible for communicating with the CSIRT (larger municipalities have more). Nearly all describe the communication between the CSIRT and the members as unidirectional. However, the members' perceptions of the information sharing with the CSIRT are distinct, due to the frequency. Some occasionally notify them if they have discovered a vulnerability they believe should be shared with others or IT or cyber-related questions. Four participants do not communicate with Health- and MuncipalityCERT, unless they are specifically asked to do so. Health- and MuncipalityCERT also inquire about feedback from the members when they send a warning to verify if the members have taken the necessary measures. The remaining section provides a list of the most to least-used communication channels in the municipality sector:

- **E-mail.** All participants concur that e-mail is their primary communication channel towards Health- and MuncipalityCERT. E-mails with vulnerability warnings are sent up to 10 times a week, usually between 2-5 times, depending on the number of relevant vulnerabilities. The warnings sent from Health- and MuncipalityCERT use TLP. All participants were familiar with this practice. They considered it as a simple, understandable protocol. The first step after receiving the warning is to deem its relevance to their internal systems. Some possess a systematic approach to verify the warnings, by using a ticketing system to resolve them.

- **Webinars.** The members frequently used the webinars, addressing IT security topics, relevant to their members. The webinars are hosted by Health- and MuncipalityCERT on their web pages monthly, and last less than an hour with a Q&A at the end.
- **Teams.** Teams is a commonly used communication channel with other stakeholders. Municipalities leveraging outsourced, security services or communication between members (e.g., KiNS, KS, and Ikomm) mention Teams as the preferred communication channel. Teams are also used for chatting and organizing digital/physical meetings with neighboring municipalities or through personal networks. Several participants considered their networks to be an important communication channel: *"I have been involved in KiNS for maybe 15 years, and getting a face and a phone number, someone you can call when you are wondering about something, is perhaps the most important thing that KiNS has given me over the years."* (**MEMB_16**).
- **VDI.** VDI is a sensor network operated by NSM, where the data is sent to the National Cyber Security Center (NCSC) analyzes and provides input for all members partaking in the network. Most of the municipalities are or wish to be a part of the network operated by NSM.
- **Other communication channels.** Two further describe other communication channels (e.g., Slack, Discord), but usually irregularly. Calling or SMS was also mentioned as an option, but few leveraged this way of communication towards Health- and MuncipalityCERT. During the operation of KommuneCSIRT, the members leveraged Mattermost.

5 Discussion

The section discusses the interview findings with the related work, and the broader European context.

5.1 RQ1: What digital communication channels are used between a sector- specific CSIRT and its members?

In the presented case, e-mail and webinars seem to be the most important communication channels used between the CSIRT and its members. The use of TLP is appreciated, as mirrored by the existing literature [17]. However, there is a concern that smaller members may regard it as spam, which also corresponds to previous findings that found small players to have a limited understanding of it [8]. Still, few actively use e-mails to share information back with the CSIRT. The presence of ad hoc communication alternatives (e.g., Discord, Teams) suggests that such channels may promote more effective communication. Other works acknowledge CSIRTs' inherent irregular nature, as they work in crisis situations [10]. Although no specific communication channels have been discussed, the importance of individual trust and informal contacts, based on formal ones, for efficient ad hoc incident response are highlighted [17,23].

Previous work [10] highlights a competitiveness between members and their fear of losing their reputation after disclosing a cyber incident. However, the interviewees in this sample facilitated for sharing of information between the members. The distinction between the literature and the empirical findings is likely due to the literature's emphasis on private companies. CSIRTs are mostly connected to the public sector in Norway, thereby having less motivation for competition. In addition, there is a concern that only a few contribute [20]. The common struggle seems to be that smaller actors share less information and thus contribute less, while larger businesses "know who everyone is" in case there is a need for coordination [8]. The findings further report that the members communicating closely with the CSIRT are the ones reporting about cyber incidents. An insecurity about which incidents should be reported to the CERT was apparent among the participants. With the upcoming NIS2 directive implemented in Norwegian sectors, along with facilitating open communication, the extent of reporting might become more clear in the future.

Several members purchase additional security services or wish to do so. However, it is unclear how the communication occurs between external security companies and sectoral CSIRTs. As there seems to be a specific wish for more SOC capabilities, they should be treated as two separate actors with defined responsibilities. Another possibility is establishing SOCs specifically tailored to one sector that could also support smaller members. Anyhow, future research should investigate how external services should cooperate with a sector-specific CSIRT.

5.2 RQ2: What factors limit information sharing between a sector-specific CSIRT and its members?

Based on the responses from the interviews, three factors seem to influence the willingness to provide information sharing with Health- and MuncipalityCERT: the size, access to critical resources, geographical location, and personal networks.

Size and access to critical resources. The larger municipalities are better equipped internally than most other municipalities, due to their size and economic status. However, it is difficult to discern from this sample as to what degree this matters to the smaller municipalities. Half of the members consist of between 200 and 5000 residents, and comparatively, this sample consists of medium to large municipalities [22]. Regardless of size, the major challenge is economic and human resources with adequate competence. Previous reports concerning cyber knowledge in the municipality sector [15] consider the municipalities to have a low maturity level. Skytterholm & Jaatun [20] discusses the same in the construction sector and calls for the establishment of an ISAC rather than CSIRTs to raise awareness and competence. Smaller players establish inter-municipality collaborations since they usually have only one individual responsible for the IT systems. Even though the size and economic status matter, no indicators of dissatisfaction with the smaller members' relationship with the CSIRT were disclosed in the case. Thus, this study can only conclude that the largest members are more willing to communicate with a CSIRT, but for medium-sized and smaller ones other factors might also play a role.

Geographical location. Participants physically close to CSIRT seem more pleased with the communication than others. The same was implied among the participants who were physically close to the former KommuneCSIRT. Belongingness is considered an important factor in cultivating effective communication. Interestingly, geographical location is less discussed in the related work. Murdoch et al. [12] mention that cybersecurity experts anecdotally report face-to-face communication as being the most valuable interaction, which necessitates physical presence. The initial face-to-face communication significantly improves information sharing but diminishes over time. However, this is only an observation based on a small sample, and may not be generalized to the rest of the population. Future work should explore how physical distance to CSIRT affects their members in another sector.

Personal networks. This factor is closely linked to geographical location, as being physically closer to each other simplifies establishing connections. The findings from this study further strengthen the need for personal networks for effective communication, as coined by previous work [8,10,12,17]. However, personal networks are also leveraged for communicating with other members. It is in the CSIRT's best interest to have its members establish personal networks with each other, as it not only promotes information sharing generally but helps the municipalities increase their resilience by having additional resources available during a potential attack and learning from each other. To benefit further from a personal network, a CSIRT could be physically available at several locations, participating more in forums, establishing a 'customer contact', or establishing visitation days.

The participants willing to be interviewed are more likely to be passionate about IT security. Due to the small sample size, it seems coincidental that few never utilized a CSIRT during an incident response. On the other hand, if this sample consists of more enthusiasts than the target population, then the participating members would be better equipped to respond to IT incidents than other members. Considering that the participants agreed on the lack of resources, it is likely that the population outside this sample faces this challenge too.

6 Concluding Remarks

CSIRTs are critical in responding to and coordinating a cyber incident. Understanding the means of communication between CSIRTs and their members could provide a swifter response, thereby limiting the consequences. This study highlighted the information-sharing practices between a Norwegian CSIRT and its members, using the municipality sector as a case. The CSIRT uses e-mail with TLP, Teams, and Discord to reach out to their municipality members. Their webinars are in general appreciated and could encourage municipalities to increase their willingness to share incidents. Still, three factors limit information sharing: size, access to resources, geographical location, and the lack of a personal network. CSIRTs may be important in an increasingly tougher cyber threat landscape, and effective communication practices toward their members may ease the understanding of possible cyber attacks.

Acknowledgments. This research has been conducted as a part of a master's thesis at NTNU, and funded by the Research Council of Norway through *Cybersecurity Barrier Management* (project no. 326717). We are grateful to the anonymous industry representatives who contributed through the interviews and discussions.

References

1. ENISA: NIS Directive, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
2. ENISA: Information Sharing and Analysis Centres (ISACs) - Cooperative models (2017)
3. ENISA: How to Setup CSIRT and SOC (2020)
4. ENISA: ENISA Threat Landscape 2023 (2023)
5. EU: DIRECTIVE (EU) 2022/2555 (2022)
6. Fujs, D., Mihelič, A., Vrhovec, S.L.: The power of interpretation: Qualitative methods in cybersecurity research. In: ACM International Conference Proceeding Series (2019). https://doi.org/10.1145/3339252.3341479
7. Ioannou, M., Stavrou, E., Bada, M.: Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In: 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). pp. 1–4 (2019). https://doi.org/10.1109/CyberSecPODS.2019.8885240
8. Jaatun, M.G., Bodsberg, L., Grotan, T.O., Moe, M.E.G.: An empirical study of cert capacity in the north sea. In: International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020 (2020). https://doi.org/10.1109/CyberSecurity49315.2020.9138865, https://doi.org/10.1109/CyberSecurity49315.2020.9138865
9. Kallio, H., Pietilä, A.M., Johnson, M., Kangasniemi, M.: Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of Advanced Nursing **72**, 2954–2965 (12 2016). https://doi.org/10.1111/JAN.13031
10. der Kleij, R.V., Kleinhuis, G., Young, H.: Computer security incident response team effectiveness: A needs assessment. Frontiers in Psychology **8**, 315125 (12 2017). https://doi.org/10.3389/FPSYG.2017.02179/BIBTEX
11. Mohd Kassim, S.R.B., Li, S., Arief, B.: Incident response practices across national csirts: Results from an online survey. OIC-CERT Journal of Cyber Security **4**(1), 67–84 (2022)

12. Murdoch, S., Leaver, N.: Anonymity vs. trust in cyber-security collaboration. In: WISCS 2015 - Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, co-located with: CCS 2015 (2015). https://doi.org/10.1145/2808128.2808134
13. NIS-direktivet (9 2014), https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/sep/nis-direktivet/id2483374/
14. NIS2-direktivet (2 2021), https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/
15. NorSIS: Kommune CERT - utredning av behov og muligheter (2015)
16. NSM: Rammeverk for handtering av IKT- sikkerhetshendelser (2017)
17. Riebe, T., Reuter, C., Kaufhold, M.A.: The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. 30 PACM on Human-Computer Interaction **5**, 478 (2021). https://doi.org/10.1145/3479865, https://doi.org/10.1145/3479865
18. Riksrevisjonen: Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor (2023)
19. Robinson, O.C.: Sampling in interview-based qualitative research: A theoretical and practical guide. Qualitative Research in Psychology **11**, 25–41 (1 2014). https://doi.org/10.1080/14780887.2013.801543/ASSET/E54A71F6-9DB1-4773-BC96-751088FB8F90/ASSETS/IMAGES/UQRP_A_801543_O_F0003G.GIF
20. Skytterholm, A.N., Jaatun, M.G.: Exploring the need for a cert for the norwegian construction sector. Springer Proceedings in Complexity pp. 57–73 (2023). https://doi.org/10.1007/978-981-19-6414-5_4
21. Software Engineering Institute: Authorized Users of the CERT Mark, https://www.sei.cmu.edu/our-work/cybersecurity-center-development/authorized-users/
22. SSB: Areal og befolkning i kommuner, fylker og hele landet (2024), https://www.ssb.no/statbank/table/11342
23. Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A.J., Repchick, K.M., Zaccaro, S.J., Dalal, R.S., Tetrick, L.E.: Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Security & Privacy **13**(4), 20–29 (2015). https://doi.org/10.1109/MSP.2015.71
24. Tjora, A.: Qualitative Research as Stepwise-Deductive Induction. Gyldendal akademisk (2018). https://doi.org/10.4324/9780203730072
25. West-Brown, M.J., Stikvoort, D., Kossakowski, K.P., Killcrece, G., Ruefle, R., Zajicek, M.: Handbook for Computer Security Incident Response Teams (CSIRTs). SEI Digital Library (2003)