Author version. Accepted for publication in Cyber Science 2022, Cardiff, Wales 20-21st June 2022. Copyright (c) Springer

Exploring the Need for a CERT for the Norwegian Construction Sector

Andrea Neverdal Skytterholm and Martin Gilje Jaatun

Abstract This paper presents an empirical study on the need for sector-specific CERT capacity in the Norwegian construction sector. Findings from the interviews demonstrate a need for developing competence on ICT security in this sector. The actors express a desire for a forum for sharing information and learning from other actors within the industry. In our estimation, there is insufficient support in the industry to create a "full-blown" CERT/CSIRT. However, it seems that all the interviewees are positive to the idea of creating an ISAC-like forum.

Key words: cyber security, incident response, incident handling, CERT, CSIRT, ISAC

1 Introduction

Digitalisation offers enormous potential for efficiency and industrialisation, and introduces new ways of working. The construction sector is an industry with many actors and a complicated value chain, making the industry vulnerable. Control of buildings, construction sites, information, and processes require digital security expertise that is highly specialized, costly, and in high demand. There is no actor today who describes a holistic situation for the industry, focusing on threats, vulnerabilities, incidents, or security measures.

Andrea Neverdal Skytterholm
SINTEF Digital, Trondheim, Norway e-mail: andrea.skytterholm@sintef.no

Martin Gilje Jaatun
SINTEF Digital, Trondheim, Norway e-mail: martin.g.jaatun@sintef.no

University of Stavanger, Stavanger, Norway e-mail: martin.g.jaatun@uis.no

The government's goal is to have response units in all sectors of society. An important task for the sector specific response unit is to ensure that all relevant actors receive correct information to be able to implement the necessary measures as quickly as possible. The sector specific response units shall be the National Cyber Security Centre's (NCSC's) contact point for ICT security incidents. Today, there is no separate sector specific response unit for the construction sector, and most actors rely on assistance from third parties to handle ICT security incidents.

This paper intends to provide an understanding of how great the need for a common collaborative security environment for the construction sector is, and what services are needed in the industry. The paper is based on interviews and a review of relevant literature and documents, along with the authors' general competence and expertise in ICT security [5, 2, 11, 12]. Seven interviews have been conducted with experts with security responsibilities from the construction sector. Also, three interviews were conducted with national emergency units for ICT security (CERT), and one interview with an ICT security services provider.

The rest of the paper is structured as follows. Section 2 present background information on the construction sector and CERT for other industries. Section 3 presents national frameworks for ICT security, and the responsibilities and tasks of sectoral response units. Section 4 presents the key findings from the interviews, and Section 5 summarises the results and identifies future work.

2 Background

Complex, comprehensive and integrated digital infrastructures and systems create new dependencies and vulnerabilities. The solutions must meet security requirements, the individual's privacy, and resilience. The less manual operations, and the more controlled by technology, the more the need for control of vulnerability and risk increases. At the same time, this means an increased need for assessment and management of threats.

Companies' IT departments are faced with new tasks and methods to be able to safeguard internal information, uptime, privacy, and effective work methodology in the company and together with other partners in the implementation of construction projects. At the same time, the threat landscape is increasing; it is now assumed that foreign intelligence services devote considerable resources to breaking into also Norwegian computer networks [13]. An increasing number of actors in different industries are experiencing attempts of external interference; state actors, contractors, organized criminals, and fraudsters are all hunting for information and attempting to exploit our infrastructure and services. Access to systems and access to premises are among the most important objectives of the threat actors [16].

The construction sector is a sector with many actors and a complicated supply and value chain. This makes the industry vulnerable. Control of buildings, construction sites, information and processes require a digital security expertise that is highly specialized, highly in demand and costs a lot. There is no actor who today describes a holistic situation picture for the industry, focusing on threats, vulnerabilities, incidents, and security measures. Nor is there a joint resource and competence centre that can support actors with notifications, information sharing or competence building. Technical analyses and technical and methodical support are up to each individual actor, without a common industry focus that can be found, for example, in KraftCERT[1], Nordic FinanceCERT[2], The Norwegian Maritime Cyber Resilience Centre (NORMA CYBER)[3] and others.

2.1 Challenges specific to the construction sector

One could argue if the construction sector is any different from other sectors regarding cyber security challenges. However, Mantha, Garcia de Soto, & Karri [7] highlight several areas where the construction sector differs from other sectors, and states some vulnerabilities that are specific to the industry:

- First of all, the supply chain of the construction sector is complex. A large portion of the construction is usually being performed by subcontractors who belong small and medium-sized enterprises (SMEs), which increases the complexity of the construction supply chain networks that is responsible for the increased cyber-vulnerability of construction process.
- The construction sites changes from project to project, which implies a dynamic workplace and workflow. The ever-changing workforce makes it difficult to educate and train employees on the best cybersecurity practices.
- There are interoperability issues regarding information needed to be shared amongst different multidisciplinary teams across various platforms.
- Exchange of confidential or sensitive information may occur outside the company's network, for instance using personal computers. Also, devices used on construction sites may not be validated or monitored by the company.
- Employees come from different socio-economic classes, they have different education levels and cultural backgrounds, which causes varying level of cybersecurity knowledge and awareness. Also, restricting access to project data by placing each employee in the right category may be challenging.

[1] https://www.kraftcert.no/english/index.html

[2] https://www.nfcert.org/

[3] https://www.normacyber.no/en/services

- Different stakeholders have different interests. Contractors are interested in maximising the profit, whereas an owner tries to minimise the total budget.
- The project teams may vary also for similar projects. This is a major limitation in the context of cybersecurity, considering that the cybersecurity policies may differ among each of the participants, and developing a synergy every time with a new set of project teams is challenging and may impact the productivity.

According to Skopik, Settanni & Fiedler information provided by national CERTs, who often take the role as contact point for coordinating and aggregating security incident reports, is usually not targeted to vertical industry sectors [14]. The authors therefore suggest that sector-oriented views, along with rich information and experience reports, are required to make CERTs more effective.

The authors of [17] describes the construction sector as a sector with complex interactions, different stakeholder interests, and lower profit margins, which make it difficult for the sector to directly adopt existing cybersecurity standards and practices from other industries. They also state that "existing cybersecurity threat models does not correspond to the life cycle phases of a construction project due to the unique communication structure and corresponding cybersecurity challenges" [17].

In [15] the authors highlight some characteristic challenges in the construction sector. They mention the changing environment and lack of stability on-site, and how this increase the challenge of providing cybersecurity during the construction phase. Besides, potential cyberattacks raises safety concerns with regards to the human interaction with machines. The authors emphasises the need for understanding potential threats agains operational technology on construction sites, detecting security vulnerabilities, and providing mitigation methods [15].

The authors of [10] have studied the lack of innovation and technological progress in the construction industry. They investigate which technologies are taken into use and the current state-of-the-art of these technologies. In the article they emphasises some challenges specific to the sector that may have had an effect on the integration of innovative technologies, such as tight collaboration with customers, subcontractors and other stakeholders, and on-site-based, complex projects which requires specialist knowledge. Besides, small and medium-sized enterprises with limited capabilities for investments in new technologies dominates the sector [10].

2.2 Working method and analytical framework

The goal of this research was to investigate the need for a sector specific CERT in the construction industry, to consider what challenges the industry

faces today, and how incidents are managed. The paper is based on interviews and review of relevant literature, and builds on our previous work [6].

We invited twenty-four actors to participate in interviews. Among these, eight actors agreed to participate. Five of the actors felt that they were not relevant participants, and two did not have the resources or time to participate. The remaining nine did not respond to our requests. See Fig. 1 for a graphical representation. One of the scheduled interviews had to be postponed, and we were unable to agree on a new interview slot.

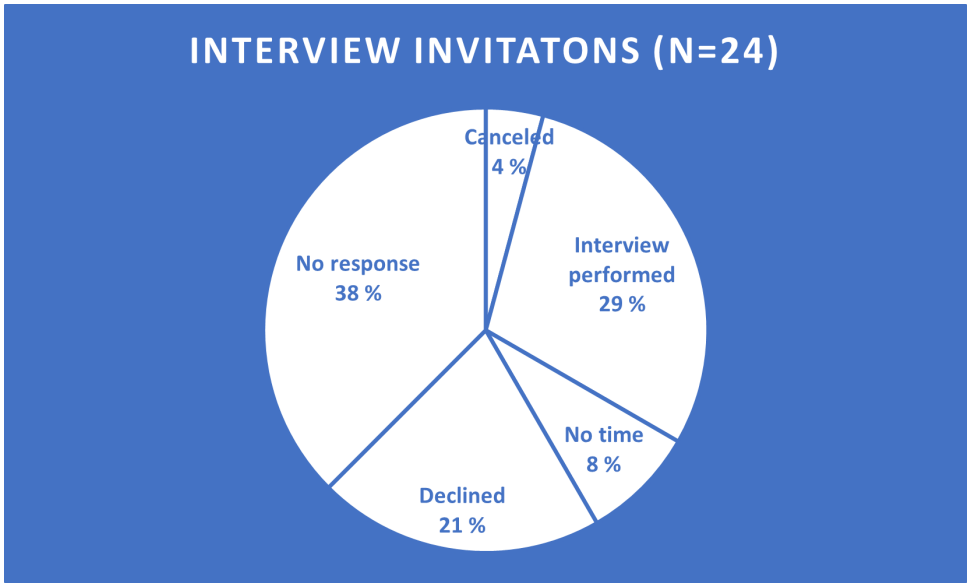

Fig. 1 Invitations to industry actors

In addition to interviews with actors from the industry, the project has interviewed three experts in national emergency response units for ICT security (CERT), as well as one provider of ICT security services. A total of 11 interviews have been conducted.

When recruiting participants to the interviews we aimed to involve people from both smaller and larger construction companies. Despite the difficulties of recruiting participants, we obtained a variation in the size of the participating companies (see Table 1).

90% of the interviewees have responsibility for the cybersecurity in the company, and the remaining 10% have a high or leading position.

All information from informants is anonymised in the paper. All information that can be associated with company names in the paper is taken from open sources.

Table 1 Number of employees at participating actors

Employees	#Actors
50	1
50-499	1
500-1499	2
1500-3500	2
3500	1

The interviews were semi-structured and an interview guide with some pre-made questions was used (see Appendix A). The interview guide was primarily used to ensure that the main topics of concern were discussed and to keep track of time during the interview sessions. We were two people conducting the interviews, where one had the role as interviewer and the other as note taker. The roles stayed the same during the entire project. After each interview we had a brief sum-up to discuss the findings and ensure that lost information was kept to a minimum.

The notes from each interview were analysed using an analysis software called Nvivo. Nvivo allowed us to encode the findings from each interview, easing the process of structuring and connecting the findings from all of the interviews. The coding resulted in four main topics which is presented in Section 4.

2.3 Limitations

As with the majority of research with busy industry practitioners, participant numbers were low. However, we experienced data saturation in the form of the actors largely agreeing on the needs of the industry and the challenges they face. Besides, triangulation with published material have helped to strengthen the reliability of the findings [17, 15, 14, 7, 10, 8, 1, 4].

The authors therefore suggest that sector-oriented views, along with rich information and experience reports could help to make CERTs more effective.

3 National frameworks for ICT security

This section presents national frameworks for ICT security, and the responsibilities and tasks of response units. Furthermore, there is an overview of Norwegian response units for ICT security, and examples of the types of tasks the different types of units have.

3.1 Framework for handling ICT security incidents

The Norwegian Ministry of Justice and Public Security has developed a framework for dealing with ICT security incidents as a key measure to contribute to strengthening the national ability to detect and deal with digital attacks [9].

The purpose of the framework is to uncover and clarify efforts between relevant actors to deal with serious ICT security incidents that affect across sectors, as well as to contribute to creating a good situational overview through aggregation and coordination of information on all relevant ICT security incidents. The framework sets requirements for the tasks that response units must take care of and what characteristics the response units must have. The framework also describes the capabilities the enterprises themselves are expected to have related to handling ICT security incidents.

The target group for the framework is public and private enterprises that are important for critical infrastructure and/or critical societal functions, sectoral response units, authorities that have a role related to the management of ICT security incidents and the ministries. The framework is not binding on private legal entities, but all ministries are encouraged to incorporate key private actors through agreements that ensure that enterprises (state administrative bodies and private legal entities) report incidents to NSM via sectoral response units.

3.2 Sectoral Response Units

The National Strategy for Information Security [8] published in 2012 assumes that the sectoral response units will play a central role in incident management. In 2016, the EU issued a separate directive (a.k.a. the NIS directive) on cybersecurity stating that Member States should ensure that they have well-functioning Cybersecurity Incident Response Teams (CSIRTs) [4]. So far, the NIS Directive has not been included in Norwegian legislation, but a limited number of Norwegian sectoral response units have been established.

The Government's goal is to ensure that there are response units in all sectors of society. An important task for a sector specific response unit is to ensure that all relevant actors receive the correct notification information in order to initiate the necessary measures as quickly as possible. The sector specific response units shall be the Norwegian Cyber Security Centre's (NCSCs) point of contact in connection with ICT security incidents.

A sector specific response unit has authority in the sector and can impose measures both in prevention and management, while the NCSC will have overall alerting and coordination responsibility. Communication with individual enterprises shall be safeguarded or coordinated with sectoral au-

thorities. The enterprises themselves have a responsibility to be able to ensure security and handle incidents.

An example of a response unit is KraftCERT which is a response function for the energy sector, but in recent years also for other industries such as water & wastewater and oil & gas. Membership in KraftCERT is voluntary, and the business must pay a membership fee.

The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015) [1] has provided a statement on cyber norms which also calls for establishing CERTs. As a confidence-building measure the States should consider additional measures to strengthen cooperation by for instance expanding the support practices in CERTs or CSIRTs such as information exchange and enhancing regional and sector-based cooperation [1].

Today, there is no formal response unit within the construction sector.

3.3 ICT Security Units (CERT)

There are a number of different response units for ICT security in Norway. Some are at the national level, some are at the sector level, some are internally in a company and some suppliers offer ICT security services within emergency preparedness. Examples of Norwegian CERT functions are given in Table 2. These are entities that are all members of the international "Forum of Incident Response and Security Teams"[4]. Below is briefly rendered example of tasks for the different types of organizations.

Based on the definition, it appears that handling incidents is the main focus of a CERT. However, the tasks of a CERT often involve far more than managing and restoring IT events. Prevention of incidents such as mapping, protection, detection and notification is often included as tasks in a CERT.

3.4 International Collaboration Forums

There are a number of collaborative forums for sharing information and experience regarding ICT security incidents.

Internationally, the term "Information Sharing & Analysis Centre" (ISAC) is used for collaboration between public and private for sharing information and experience from combating and handling ICT security incidents. An ISAC can be specific to a sector. EE-ISAC is an example of a European cooperation forum that includes several European energy companies. FIRST is a global member forum for collaboration between trusted CERT actors. The

[4] https://www.first.org/

Table 2 Norwegian actors that are members of FIRST

Short name	Full name	Host organisation	Type of organization
BF-SIRT	Basefarm SIRT	Basefarm AS	Data center/ cloud service vendor
Defendable CERT	Defendable CERT	Defendable AS	ICT security service vendor
DNB CDC	DNB Cyber Defense Center (IRT)	DNB ASA	Finance sector
EkomCERT	Nkom EkomCERT	Norwegian Communications Authority (Nkom)	Public body
Equinor CSIRT	Equinor Computer Security Incident Response Team	Equinor ASA	Energy sector
HelseCERT	HelseCERT	Norsk Helsenett SF	Public body
KCSC	Kongsberg Cyber Security Center	Kongsberg Defence and Aerospace	Industry sector
KraftCERT	KraftCERT	KraftCERT AS	Energy sector
mIRT	mnemonic Incident Response Team	mnemonic AS	ICT security service vendor
NCSC-NO	National Cyber Security Centre in Norway	Norwegian National Security Authority	Public body
Nordic Financial CERT	Nordic Financial CERT	Nordic Financial CERT association	Finance sector
Norges Bank CSIRT	Norges Bank CSIRT	Norges Bank	Finance sector
Tax-IRT	The Norwegian Tax Administration Operational Security Team	Skatteetaten	Public body, Finance sector
TCERT	Telenor CERT	Telenor Norge AS	ICT/Telecom
UiO-CERT	University of Oslo Computer Emergency Response Team	University of Oslo	Research and education
UNINETT CERT	UNINETT CERT	UNINETT AS	Research and education
Sopra Steria SOC Nordics	2S-SOC	Sopra Steria AS	ICT service vendor, including security
SpareBank 1 IRT	SpareBank 1 Incident Response Team	SpareBank 1 Utvikling DA	Finance sector
Visma CSIRT/CC	Visma Cyber Security Incident Response Team / Coordination Center	Visma AS	Software vendor

forum currently has 605 members. Norwegian members of FIRST are shown in Table 2

4 Results from interviews

We have conducted online interviews with experts with security responsibilities from the construction sector from five contractor companies, one engineering and advisory company and a builder and property manager. In addition, we have spoken to three experts from different national CERTs, as well as a provider of ICT security services. In this section we present the results of the interviews categorised into four main topics. The interviews took place in the period September-November 2021.

The interview guide used in interviews with industry actors is given in Appendix A.

4.1 Vulnerabilities

Seven informants define an ICT security breach as unauthorized access to data. One of the informants uses a slightly different definition, where an ICT security breach is described by employees losing one of their devices without notifying them, sharing their password with others or observing something suspicious without notifying.

Three of the actors have agreements with Microsoft that notify them if something abnormal is detected in their systems, and this is one of the ways security breaches are usually detected. Security breaches are also reported by employees or users who, for instance, have been granted access to systems or documents they should not have access to. Seven out of eleven respondents also receive notifications from third parties that monitor network traffic to and from their systems.

From the interviews, it is not clear what is the most frequent cause of security breaches. All the actors we spoke to could refer to ICT security breaches of varying severity, to which either they or their supplier have been exposed.

One of the actors says that they have been subjected to numerous attacks, and that the attackers often make use of "social engineering" and go through employees. Employee behaviour is therefore something they focus on. Many of the attacks are also often about financial crime. Another actor also told about a security breach where Social engineering was used as an entry gate.

Three of the actors have experienced being exposed to, or had, a provider that has been exposed to ransomware. One of the actors report that they received extortion claims, but that they did not pay them. They had a backup

of the systems, and wouldn't have come back any faster if they had paid the claim. It is not evident what was the entry gate for the ransomware.

4.2 Incident management

There is a large gap between the internal IT resources among the actors. For example, one of the actors has no internal IT resources, only one self-appointed IT administrator, while another actor has an internal IT department with different service owners in charge of their services, and uses third-party providers for advice. Common to all of the actors is that they use third-party providers to handle ICT security incidents. All the actors who tell about specific ICT security incidents confirm this. Some of the actors have fixed agreements with their supplier, while one actor reports that they have no fixed agreements, but only contact a supplier when they need assistance. According to one of the actors we have spoken to, a normal Norwegian company will not have the expertise needed to restore the systems in the event of an ICT security incident, and that they must therefore hire specialist expertise anyway. Through our interviews, we have not uncovered actors experiencing challenges in cooperation and coordination of handling ICT security breaches.

4.3 Challenges facing the industry

One of the challenges mentioned by 50% of the actors is that the industry is immature. Through interviews, we have the impression that the maturity when it comes to cybersecurity/ICT security in the industry varies, both between the actors, but also within the companies. One of the actors mentions that the competence of the management is good, and that they understand the importance of implementing security solutions, while outwardly in the lines it is inferior. It is difficult for management to communicate the importance of, for example, two-factor solutions. Employees don't understand why it's necessary, and they find it cumbersome. Another actor says that they had no challenges in adopting this, because people are used to using it. A lack of IT expertise, both in terms of outdated and newer IT systems, is also a challenge. It is often difficult to obtain expertise in the older and outdated systems, as this competence sits in the head of an ageing workforce. It is often the younger ones who have expertise in the newer IT systems, but also here many do not have this expertise.

Another challenge mentioned by almost 40% of the actors, and can possibly be seen in the context of the point above, is that there are many who do things themselves, without thinking about what consequences it can have. Intervie-

wees mention for instance that some of the solutions are a bit "cowboy-like", and that they have, among other things, seen remote control systems that have been quite accessible to outsiders, or that servers have been placed in a building without securing them.

Having control over the suppliers and ensuring that they have ensured safety in a good way can be a challenge, and the actors therefore depend on having a strict structure here. When the Internet of Things (IoT) is used in barley, it is important to ensure safety so that these are not used as a backdoor into their systems.

4.4 Sector CERT

All the representatives who participated in the interviews say they would benefit from an industry-specific CERT. Two of the actors say that it might be appropriate to replace the Security Operations Center (SOC) that they have today with an industry-specific CERT, but that this depends, among other things, on technology, price and functionality. The other actors seem to have the greatest need and interest in a forum where one can share experiences and information.

Today, none of the actors share information about incidents among themselves, but everyone agrees that they had benefited from a forum for information sharing with other actors. Information they would like to share deals with, among other things, ICT security incidents, industry-specific vulnerabilities and industry-specific solutions to address these vulnerabilities, and also to raise awareness in the industry. Some also mention that they want a forum where they can share experiences and learn from each other.

Of the actors we spoke to, only one of them had been in contact with a CERT channel in connection with the handling of an incident. Due to receiving assistance from a supplier, the CERT channel considered that no further support was required from them. However, they had sporadic contact along the way, even though they were not actively involved in handling the incident. The actor was interested in knowing if the attack was one of many, or if it was targeted at them, but this could not be answered for sure, but they assumed that it was not targeted as they see that the frequency of such types of attacks is increasing.

As it is today, several of the CERTs may be relevant for some of the actors. The problem is that it can be difficult and unclear who to contact and in what situations. Some believe that this problem speaks against having an industry-specific CERT, as it makes it even harder to know who to deal with in different situations. On the other hand, the construction sector is large, and there is currently a lot going on on the technology side, which suggests either establishing an unit, or participating in existing units (CERTs).

The method used to attack systems in the construction sector is no different than if one were to attack another industry. One of the respondents could not see anything that makes the construction sector any more special than other response units that exist.

The price for hiring consultants to assist in dealing with ICT security incidents is already high. One of the actors says that it is difficult to understand how one should have managed to finance such a team that is ready to assist around the clock.

Another drawback mentioned is that IT security is already highly in demand, and that it will be difficult to get enough people with that expertise to be able to operate an industry-specific CERT.

One of the actors acknowledges that there may be challenges in bringing people along, and that it is not only two or three actors that contribute to the sharing of information. Through our interviews, however, it has emerged that all actors are positive about information sharing. One of the actors also says that there is no reason not to cooperate in this area. They are competitors, but sharing this type of information will not come at the expense of the competition between them. When it comes to information sharing about their own ICT security breaches, they have a common interest in hearing about each other's events.

From interviews with authorities and other CERT channels, it has emerged that creating an ISAC can be a good start. It is also easy for an ISAC to have a connection to the technical unit of NSM, and this contact they can have regardless of whether they are an ISAC, sector response unit or CERT, the only thing that changes is the requirements set by the NCSC. One of the established CERT's says that it is important to get a forum on security, regardless of whether it is a sector response unit or an ISAC.

The CERT channels we have been in contact with do not make any recommendations on whether or not an industry-specific CERT should be created. The most important thing is that the actors have a place where they can share and get information. If they only work alone, they will become a much easier prey for attackers. Whether this place is one of the established CERTs or if it is something industry-specific does not have much significance.

None of the actors we have spoken to use the traffic light protocol (TLP). Those familiar with the protocol have become familiar with it through reports or security assessments from others. One of the actors mentions that they have used TLP in internal risk assessments.

5 Summary and conclusions

The summary and conclusions below are based on the main impressions from the interviews with actors in the construction industry, national emergency

response units for ICT security (CERT) and a supplier of ICT security services.

5.1 The needs of the industry

There is a large degree of variation in internal IT resources among the participants who have participated in the study. Common to all of them is that they use suppliers to handle ICT security incidents, either through fixed agreements or by contacting suppliers when an incident occurs. According to one of the respondents, a normal Norwegian company will not have the expertise needed to restore the systems in the event of an ICT security incident, and that they will therefore have to hire specialist expertise to assist with the handling anyway.

Only one of the actors we have spoken to has an internal IT department that participates actively in handling incidents. This actor also uses suppliers to assist with incident management. From the interviews, there is nothing to indicate that a large actor with an internal IT department is able to handle ICT security incidents better than a small actor who only uses suppliers to handle the incident. The price for supplier services, on the other hand, is high, so the capacity of the actors to pay for these services will probably vary. If the incident is large enough, and it takes a long time to deal with it, then the differences between small and large enterprises may become clearer.

It seems that all the actors we have spoken to are pleased with how the incidents are handled today, and they make use of suppliers who assist with incident management. Based on this, we do not see a need for a separate response unit. On the other hand, some of the major actors would consider replacing the supplier/SOC that they use today in favour of an industry-specific CERT.

All the actors express that they would benefit from a forum to discuss industry-specific threats, incidents and security solutions, all of which are positive about information sharing. This can be a low-threshold measure that can either be operated on the basis of the larger construction sector actors, or by the actors joining forces on the "perform to capacity" principle to pay an external organisation to do so.

Interviews and experiences from other projects show that the construction sector is relatively immature, and that there is a high degree of variation in competence when it comes to cybersecurity/ICT security. There is a need for competence enhancement in this area throughout the industry. However, the findings also indicate that the construction sector is concerned with cybersecurity/ICT security, and wants an ISAC in order to raise competence in this area.

There are several challenges in creating a separate response unit for the construction sector. The cost of hiring consultants to assist in dealing with

ICT security incidents is already high, and one of the respondents says that it is difficult to envisage that a team that is ready to assist around the clock should be managed and funded. IT security is a highly sought-after expertise, and it is mentioned that it will be difficult to get enough people to be able to operate an industry-specific CERT. Another challenge mentioned is that it can be difficult to bring enough actors to such a unit, and also that everyone contributes information. There are currently several existing CERT units that may be relevant for the actors, but it can be difficult and unclear which of them to contact in different situations. Some believe that this problem speaks against having an industry-specific CERT, as it makes it even harder to know who to deal with in different situations.

From interviews with authorities and other CERT channels, it has emerged that creating an ISAC can be a good start. It is also easy for an ISAC to have a connection to the technical unit of NSM, and this contact they can have regardless of whether they are an ISAC, sector specific response unit or CERT, the only thing that changes is the requirements set by the NCSC. One of the established CERTs says that it is important to get a forum on security, regardless of whether it is a sector specific response unit or an ISAC.

5.2 Organization of an ISAC

To run an ISAC, one needs a secretariat that is responsible for, among other things, organizing meetings and running a digital platform for information sharing. The secretariat responsibility can be rolled out between the members or it can be serviced to an external actor. Members of an ISAC must expect to set aside about two days a month. These days are used to participate in meetings, contribute information sharing on a digital platform, and participate in collaborative activities such as organizing campaigns, developing products or tools, and conducting sector analysis. When starting up an ISAC, it is recommended to start with few actors, to build relationships and trust. These relationships can also be used to create trust among several members. It is recommended that the membership size does not exceed 20-25 members, as many members can make the administration of the ISAC difficult [3]. Representatives from member companies should have sufficient expertise to provide information and benefit from discussions, and they must have the authority to represent the company and speak freely during the meetings. In addition, they must be able to contribute, or receive information at a relevant level (for example, strategic vs. technical level).

Acknowledgements

This work is based on research funded by Oslo Construction City AS. The authors gratefully acknowledge the support from Obos, AF Gruppen, Betonmast and Statsbygg, and the anonymous interviewees from the participating organisations.

References

1. Assembly, U.G.: Group of governmental experts on developments in the field of information and telecommunications in the context of international security. UN Doc. A/70/174 **22** (2015)
2. Bernsmed, K., Jaatun, M.G., Meland, P.H.: Safety critical software and security-how low can you go? In: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), pp. 1–6. IEEE (2018)
3. ENISA: Information sharing and analysis center (isacs) – cooperative models (2018). URL `https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models`
4. European Union: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union (2016). URL `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN`
5. Jaatun, M.G., Bodsberg, L., Grøtan, T.O., Moe, M.E.G.: An empirical study of cert capacity in the north sea. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8. IEEE (2020)
6. Jaatun, M.G., Bodsberg, L., Grøtan, T.O., Elisabeth Gaup Moe, M.: An empirical study of CERT capacity in the North Sea. In: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–8 (2020). DOI 10.1109/CyberSecurity49315.2020.9138865
7. Mantha, B., de Soto, B.G., Karri, R.: Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society **66**, 102682 (2021)
8. Norwegian Government: Nasjonal strategi for informasjonssikkerhet (*National Strategy for information security* [In Norwegian]) (2012). URL `https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal\_strategi\_infosikkerhet.pdf`
9. NSM: Rammeverk for håndtering av IKT-hendelser (*framework for handling ict incidents* [in norwegian]) (2017). URL `https://nsm.no/getfile.php/133853-1593022504/Demo/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf`
10. Oesterreich, T.D., Teuteberg, F.: Understanding the implications of digitisation and automation in the context of industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. Computers in industry **83**, 121–139 (2016)
11. Okstad, E.H., Bains, R., Myklebust, T., Jaatun, M.G.: Implications of cyber security to safety approval in railway (2021)
12. Onshus, T., Bodsberg, L., Hauge, S., Jaatun, M.G., Lundteigen, M.A., Myklebust, T., Ottermo, M.V., Petersen, S., Wille, E.: Security and independence of process safety and control systems in the petroleum industry. Journal of Cybersecurity and Privacy **2**(1), 20–41 (2022)

13. PST: National threat assessment 2020 (2020). URL https://pst.no/alle-artikler/trusselvurderinger/annual-threat-assessment-2020/
14. Skopik, F., Settanni, G., Fiedler, R.: A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security **60**, 154–176 (2016)
15. Sonkor, M., de Soto, B.G.: Is your construction site secure? a view from the cybersecurity perspective. In: ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction, vol. 38, pp. 864–871. IAARC Publications (2021)
16. Telenor: Trusselrapport 2020 - Trusselforståelse (*Threat report 2020 - Threat perception* [In Norwegian]) (2020). URL https://www.telenor.no/om/digital-sikkerhet/2020/artikler/trusselforstaaelse.jsp
17. Turk, Ž., de Soto, B.G., Mantha, B.R., Maciel, A., Georgescu, A.: A systemic framework for addressing cybersecurity in construction. Automation in Construction **133**, 103988 (2022)

Appendix A

Interview guide

Background

- What is your role in the company?
- Can you describe how your role is linked to managing ICT security incidents?
- Is the term Operational Technology (OT) used in your company?

CERT capacity in the construction sector

- What systems and routines fall under your responsibility? CERT capacity in the construction sector
- What do you consider especially challenging in your sector regarding protection against and managing of cyberattacks/ICT security incidents?
- What internal resources and roles are involved in ICY preparedness and incident management in your company?
- How do you define an ICT security breach?
- How are ICT security incidents usually discovered in your company?
- Do you have any plans for managing ICY security incidents?
- Are these plans included in trainings and exercises?
- Who is contacted in the event of serious ICT security breaches? When did you last update your contact lists?
- How do you collaborate with other actors on handling ICT security incidents?
- Do you see special challenges related to dealing with ICT security breaches in industrial process control systems and automation?

- Would you benefit from a sector CAC for your industry to better understand, detect and deal with threats and vulnerabilities? If so, how would you benefit from such a CAC?
- What improvement needs do you think are the most important when dealing with ICT security breaches in your case?
- Can you tell us about the last ICT security breach you experienced?
- How was this handled?
- How did the handling work?
- Why did the handling work as it did?
- Do you experience challenges around cooperation and coordination of handling ICT security breaches? If this is the case, what kind of challenges are experienced?
- Would you benefit from participating in national exercises focusing on handling ICT security incidents? Feel free to elaborate on why

Operationalization of CERT alerts

- How is your practice regarding information sharing about (own) ICT security breaches? What type of information is shared, and with whom?
- What tools are used for information sharing about ICT security breaches in your company?
- Do you know the term TLP (traffic light protocol)? If so, how is this used in your company when sharing information?
- Do you share information about your own ICT security breaches via CERT channels? If so, what type of information, and in what way?
- Do you receive information about new ICT security threats and vulnerabilities via CERT channels? If so, how is this information used in the company's internal ICT security and emergency preparedness work?
- What improvement needs do you think are the most important when it comes to sharing information in ICT security incidents and operationalizing CERT alerts?

General closing questions

- Are there topics we have not addressed in this interview that we should have addressed?