An Empirical Study of CERT Capacity in the North Sea

Martin Gilje Jaatun, Lars Bodsberg and Tor Olav Grøtan
Software Engineering, Safety and Security
SINTEF Digital
Trondheim, Norway
{martin.g.jaatun, lars.bodsberg, torog} @sintef.no

Marie Elisabeth Gaup Moe[§]
IIK
NTNU
Gjøvik, Norway
marie.moe at ntnu.no

***Abstract*—This paper documents the results of an empirical study of cyber incident response readiness in the Norwegian petroleum industry. The study addressed the Computer Emergency Response Team (CERT) capacity among various actors in the industry in handling critical cybersecurity incidents in industrial control and safety systems, with a focus on Operational Technology (OT) systems. The paper presents results from interviews with personnel in petroleum companies as well as interviews with national and international CERT actors. The informants in the petroleum industry are relatively satisfied with their own CERT capacity today, but it is acknowledged that one can always improve. Oil and gas companies and drilling companies share information and experience in various (virtual) meeting places and forums organized by external actors, but there is little focus, especially among the smaller companies, on systematic sharing of information and experiences of cyber incidents. There is a strong need for coordinating and harmonizing cybersecurity in IT and OT systems, as there are significant differences in terminology, maturity of technical solutions and culture today. CERT actors pointed out a need for better communication and contact between CERT actors and key persons within the companies, something that could be accomplished with the establishment of a petroleum sector Information Sharing and Analysis Centre (ISAC).**

I. Introduction

The petroleum industry is increasingly reliant on digital systems, and companies have ambitious plans for increased use of digital technology for production optimalization and cost reduction. Digitization involves the introduction of digital technologies such as data methods and tools to replace, streamline or automate manual and physical tasks. This will potentially have clear benefits for Health, Safety and Environment (HSE) and contribute to greater competitiveness. This development however, also leads to new challenges related to cybersecurity. The industry must therefore actively follow up changes in the risk landscape due to more complexity and connectivity of systems, and increased exposure to continuously evolving cyber threats.

For example, in 2017, a new sophisticated and serious cyber attack was discovered to be aimed at industrial control systems (ICS), affecting critical safety systems. It was discovered by the provider Schneider Electric and analyzed by the cyber security firms Fireeye [1] and Dragos [2]. The malware known as Triton/Trisis triggered an emergency stop in the Triconex safety system for industrial process control systems. This incident reminds us that industrial control and safety systems are also vulnerable to cyber attacks, and that a cyber attack against ICS could have potentially physically damaging and catastrophic consequences. In 2019 Dragos published a whitepaper [3] assessing cyber threats affecting the global oil and gas sector. In their report five different threat actor groups are identified as targeting the petroleum sector. Out of these five the Xenotime group that uses the Triton/Trisis framework is deemed as the most prolific threat actor, with ICS-specific capabilities and access to tools that could cause disruptive incidents. An overview of the threat picture against the Norwegian petroleum sector in a geopolitical context is given in a recent NUPI report [4].

A. A Short History on Computer Emergency Response

The first Computer Emergency Response Team (CERT) emerged in the aftermath of the Morris Worm [5], as Carnegie Mellon University (CMU) received DARPA funding to establish what eventually became the CERT Coordination Center (CERT-CC). The need for a CERT was demonstrated by the complex communication and negotiation requirements associated with handling the Morris Worm incident, and the challenges of restoration efforts afterwards. The CERT term is a registered trademark of CMU, and all organisations wishing to use it must have a license from CMU to do so. Partly for this reason the alternative term Computer Security Incident Response Team (CSIRT) became popular, and currently some teams call themselves CERT, while others use CSIRT, without there necessarily being a discernible difference.

Computer Security Incidents can be a fascinating area of study, but unfortunately corporate secrecy and confidentiality requirements often make it very difficult for researchers to get access, and there is relatively little academic research available [6].

A CERT will normally deal with an incident as it happens, but this is often just a small part of what it does; looking at the five-phase model of ISO/IEC 27035 [7], most of the time is actually spent in the ”Plan” phase [8]. A CERT is often tasked with duties such as awareness-building and training, including building ties to national and international communities. Most tertiary education institutions have their own CERT, and there

[§] At the time of the study, Dr. Moe was employed at SINTEF Digital are various sector CERTs (e.g., health, finance) in addition to national CERTs (in Norway: NorCERT[1]).

B. Empirical Contribution

This paper documents the results of an empirical study of cyber incident response readiness in the Norwegian petroleum industry. The study addressed the CERT capacity among various actors in the industry in handling critical ICT security incidents in industrial control and safety systems, with a focus on Operational Technology (OT) systems. Main research questions have been: How are ICT security incidents managed? How do actors collaborate in managing ICT security incidents? What is the current practice for information sharing about ICT security incidents? What are the main challenges in managing ICT security incidents?

The study is neither a case study or a systematic survey, but offers a snapshot of the current state of affairs related to how a number of different actors perceive the current CERT capacity in the sector, how the different actors experience themselves and each other, and, to some extent, what are pathways for improvement. The sample of interviews is small, but at the same time the actual population of actors is also rather small. Resting on the confidence implied by the selection of interviewees by the Norwegian Petroleum Safety Authority (PSA), the study offers a best available representative picture across a population of small and large actors, and across ”insiders” and ”outsiders” relative to the industry and its specific OT challenges. We choose to denote our presentation of this composite set of sources with various proximity to the OT problem domain an ”impression”, to signify that it does no not carry the scientific rigour of a survey or case study in the classical sense. However, we think that this impression, also based on a contrasting with other sectors, still is a valuable asset for advancing the complex task of finding effective CERT approaches in this domain.

The paper presents results from interviews with personnel in petroleum companies involving 12 subject area experts in 2 oil and gas companies and 2 drilling rig companies. These companies were included based on input from the Petroleum Safety Authority. In addition, the project has interviewed 8 subject matter experts in national and international “CERT actors” such as National Cyber Security Centers (NCSCs), CERTs and private companies offering products and services within ICT security. The informants include four CERT managers, CERT members who work with incident management, NCSC advisors and management, a security advisor, a security consultant, and an incident management manager.

All interviews are based on a common semi-structured interview guide and lasted between one to two hours. This means that the interviewee has been given a guideline for the interviews, but some questions have been added during the interview, depending on which theme the informers have raised. Vendors of industrial control systems have not been part of the study. All information from informants has been anonymized; any information herein that can be associated with company names is collected from open sources. In general, we find little information about CERT capacity in the petroleum industry through searches of publicly available information on the Internet.

II. CERT Capacity in the Petroleum Industry

In the following we present our main impressions about CERT capacity from interviews with companies in the petroleum industry.

A. Current State of Response Readiness

It seems in general that the informants are reasonably satisfied with the current state of practice. However, the size of the companies has, not surprisingly, a big impact on the answers [9]. Large companies have more in-house cyber incident response capacity than small companies.

Several point out that the security expertise of suppliers could be better; this is often mentioned in the context of a general under-capacity of cybersecurity expertise in the company’s industry (or community). According to one informant, ”We are starting to create a document to send to our vendors of ICS systems. This helps to separate the cyber security from getting muddled with other parts. This is to put pressure on manufacturers to focus more on cyber security (via procurement). We want this to be a standard, and not something that each individual contractor looks into.”

An observation from the interviews is that companies do not perceive the absence of an ”oil CERT” for reactive incident handling to be much of a problem, but many of the interview subjects are positive to the notion of having a sector-based proactive ”CERT-like” organization for sharing of information and experiences related to cyber incidents. This could be realized as a dedicated petroleum sector Information Sharing and Analysis Center (ISAC). There are meeting places today based on personal relationships; the larger players have contact with international communities, while the smaller ones appear to rely a lot on security service providers. The smaller companies that have foreign parent company with their own CERT (or similar), seem to have varying degrees of interaction with their parent company CERT.

We find that dedicated tools for information sharing are used only to a small extent; communication is mostly done via email and phone. Some mention NorCERT (the national CERT of Norway) encrypted Internet Relay Chat (IRC), but this is still text-based, in free form. Several mention Malware Information Sharing Platform (MISP)[2] as a platform for exchanging indicators of compromise (IoC) such as IP addresses and signatures, but the impression is that information sharing on this platform is perceived as more relevant to cyber threats against IT systems, not OT systems.

Several informants mention ”information overload” as a problem with regard to information on vulnerabilities and attacks, both from CERT actors and other sources - this also

[1] https://www.nsm.stat.no/norcert

[2] https://www.misp-project.org

applies to those who obtain information from an internal CERT in the parent company abroad. Several informants have identified a need to have a form of automated filtering of the information so that anything that is not relevant to the individual company is removed before it is presented. This would require that each company has a configuration and inventory management system that can provide a complete overview of all equipment with associated software and updates. It does not appear that any of the players have such a complete system today.

All informants say they have their own guidelines/procedures for cybersecurity; these are in varying degrees based on international standards (e.g., [10], [7], [11], [12]), but the informants are generally not concerned with these standards, instead keeping the focus on the internal guidelines.

All informants argue that they have good cooperation with other actors operating in the petroleum industry in the North Sea, and that ”we know who everyone is” in case there is a need for coordination. However, the smaller players appear to not really share much information about handling cyber incidents with each other, and certainly not during the active incident handling phase. The informants refer to various meeting places (partly organised by external actors such as NorCERT or vendors), but this is not related to active incidents or crises.

There is a great deal of variation in the perception of the difference between IT and OT systems, and who should be responsible for which systems. The extent to which the informants perceive that they are capable of dealing with cyber security events in OT also varies. Several informants point out that increased use of real-time detection and monitoring of security breaches in OT systems will be useful. Similarly, many informants perceive that when security breaches are detected, it may not be possible to shut down OT systems in the containment phase of incident response, e.g. to perform emergency security updates.

B. Operationalization of CERT Alerts

Operationalization of CERT alerts was particularly addressed in the study as information sharing is an important component of incident management of cyber attacks. CERT actors regularly prepare alerts for new vulnerabilities and incidents. When a new type of malware is detected, the CERT shares information from vendors, alerts about countermeasures, and how the malware can be detected and removed.

During the handling and analysis of an incident, information called ”Indicators of Compromise” (IoC), including different types of ”artifacts”, are collected from the forensics and malware analysis. This can be

- IP addresses and domains the malware sample contacts (the malware ”calls home” to a command and control server to receive instructions or download additional malware modules)
- IP addresses and domains from which ”phishing” emails are sent
- Filenames and hash values of files that the malware or attacker installs on the system
- Other typical characteristics of the malware or observed network traffic patterns
- Info about the attacker’s ”modus operandi”, footprint, tools and tradecraft

These IoCs are shared with other CERTs, as well as sent to companies that are on the CERT’s distribution lists, often in an ”anonymized” form where the identity of the victim of cyber attack is not disclosed. For each CERT alert it is also considered which other national and international CERTs that should be given information.

Some examples of information sharing paths for alerts include:

- From NorCERT to the internal response team of an organization,
- From NorCERT to a sector CERT and on to the internal response team of an organization, and
- From a foreign national CERT to NorCERT, to a sector CERT and then to the internal response team of an organization.

C. Traffic Light Protocol Practice

The purpose of CERT alerts is that the recipient should be able to utilize the information to secure their systems or discover and handle attacks. This assumes that they have a defined scheme for receiving alerts, and internal systems and processes where the information is further processed. IoCs or information about new vulnerabilities could be used to update firewall configurations, add signatures to an intrusion detection system (IDS), or search for suspicious network activity or entries in system logs, and other ”threat hunting” activities. An organization that operationalizes this in its internal processes, will be able to improve its security and ability to detect and respond to cyber attacks. If such an operationalization is not in place, CERT alerts will become redundant information and only help fill up the inbox of the the person receiving notifications.

Without trusted cooperation, partnerships are breaking down, which leads to lack of information sharing within the CERT community and from the intelligence services, thereby missing information distribution to CERT members. A prerequisite for successful sharing of potential sensitive incident information is that the reporting entity can rely on the CERT to only share further information that is absolutely necessary. This means that some information sharing must be strictly on a need-to-know basis.

It is especially important that the threat actors do not get acquainted with the information and thereby adopt the malware or refine their attack methodology to bypass countermeasures. The Traffic Light Protocol (TLP) is a standard for information sharing that ensures that the information owner has control over who receives information and how it is shared. Table I displays the levels in the TLP protocol.

CERT alerts for new vulnerabilities intended for a larger audience are most often shared with TLP GREEN or WHITE.

TABLE I
TRAFFIC LIGHT PROTOCOL (ADAPTED FROM FIRST)

TLP level	**Explanation**
TLP:RED	No information sharing beyond recipient. Information may damage your privacy, reputation or operation if it is misused.
TLP:AMBER	Information may be shared internally by the recipient's organization or partner. The information may damage your privacy, reputation or operation if it is misused.
TLP:GREEN	Information can be shared with other players within the sector. The information is useful for the awareness of all participating organisations and the general information security environment.
TLP:WHITE	No restrictions on information sharing. The information entails minimal or no anticipated risk of misuse in accordance with the current rules of publishing.

CERT alerts containing IoCs obtained in incident handling of targeted attacks are often shared as TLP:AMBER. For highly sensitive information, information is shared orally in closed meetings under TLP:RED.

There is still some confusion surrounding the definition of TLP:AMBER. In the original definition, sharing was limited to within your own organization. Standard practice for TLP:AMBER is therefore to add a specification of who the information can be further shared with.

D. Current State of Information Sharing and Operationalization of CERT Alerts

Based on the interviews, the main impression is that there is great variety among the actors in the industry to what extent the actors have operationalized CERT alerts in their internal processes and tools. Some informants perceive that CERT alerts are not very relevant to themselves and their industry, and call for better filtering of the information. Informants who do not communicate directly with a CERT express that they have not received CERT alerts, nor have they heard of TLP. Several see the need for more information sharing, and are positive to the idea of an ”oil ISAC” that focuses only on information sharing, rather than an ”oil CERT” that also contributes to incident management.

Information sharing happens most often via email, but some also use information sharing platforms. The Malware Information Sharing Platform (MISP) is mentioned by several actors. Some have also developed their own information sharing platforms adapted to internal tools and processes. Synergi[3], which is a general system for governance, risk management and compliance, more often used for reporting of Health, Safety and Environment (HSE) incidents, is also used by some organizations for reporting of cyber security incidents.

Chatting on NorCERT's IRC channel is mentioned as a useful source of information for those who participate in the national intrusion detection network for critical infrastructure VDI[4]. It seems that few companies have a focus on gathering IoCs from their own incidents and sharing them with other actors in the industry; this seems to be a topic exclusively considered by the CERTs that were interviewed.

Classified information according to the Security Act can be a challenge when the players communicate with NorCERT. Some have experienced that information that they themselves have collected on unclassified systems – and which they believe should have been unclassified – later was returned to them from NorCERT as classified information. ”Overclassification” of information can be a problem when collaborating with public CERT-actors. One possible solution is to sanitize the information so that it can be shared according to TLP. IoCs can for example be shared as TLP:AMBER if classified information about the threat actor that is behind the attack is removed.

Some international CERTs have facilitated liaisons from the industry to be physically present at their premises. This will be personnel with security clearances who act as focal points against the various sectors, contributing to network building and information sharing with the private actors.

Our impression is that the small players have very limited understanding of the Traffic Light Protocol (TLP), and that those who receive TLP-marked information will hesitate to pass it on to anyone, even if the marking permits this.

III. CERT SOLUTIONS IN OTHER SECTORS NATIONALLY AND INTERNATIONALLY

In the follwing, we summarize the main impression from interviews with CERT actors in other segments than the petroleum sector related to information sharing, monitoring and reporting of cyber incidents, security exercises, and detection and handling of security breaches.

A. Information sharing

1) Trust: The interviews show that the CERT actors rely on personal networks in information sharing. That is, access to information depends on who you know. Several informants mention the importance of trust, and that trust is created through personal networks for information sharing. ”Trust is the most important thing”. It's easier to share sensitive information with others that you know personally. Some email

[3] https://www.irmsecurity.com/cyber-solutions/synergi-grc-platform/

[4] https://www.nsm.stat.no/NCSC/NCSS-hendelser/varslingssystem-for-digital-infrastruktur-vdi/

lists and informal networks for information sharing are also based on personal invitations.

Within OT, it is difficult to know who to contact since the industry is quite small. Even after a serious incident, antivirus companies, suppliers or other third parties are not necessarily involved.

Trust is perceived as a prerequisite for intelligence services to share information with CERT actors, such as using TLP:RED (ref. Table I). Another reason why trust is experienced as a central part of information sharing is that collaboration between industry actors and organisations such as NCSCs, CERTs and ISACs is often voluntary.

2) Commitment to share: Voluntary information sharing can be challenging as businesses are not obliged to share, even though information may be important to others. This challenge applies nationally as well as internationally.

Regulation is a means to ensure that important information and incidents are reported. For example, in Norway, companies associated with KraftCERT[5] will be required by statute to report all security incidents. Any further reporting by KraftCERT to, for example, NorCERT, may only be performed with the agreement of the company.

In today's regulations within the petroleum industry, there are requirements for immediate notification to the Petroleum Safety Authority in the event of danger and accident situations that have resulted in, or could have resulted in, a serious weakening or loss of safety-related functions or barriers, so that the integrity of the facility is at risk (Section 29 of the PSA management regulations [13]). According to the guide, situations where normal operation of control or security systems are disturbed by unscheduled work (ICT event) should be reported.

3) Cross-border Cooperation: CERT collaboration and information sharing are related to geography. One interviewee mentioned a security incident which was not reported to the CERT in the country in which it occurred, but was only reported to the CERT in the country in which the company is headquartered, and never reported back to NorCERT or any other Norwegian CERT (see Fig. 1). Insufficient information sharing across borders can thus cause the national CERT to not have an overview of all events in its own country.

When it comes to international CERT cooperation, it is particularly difficult to deal with a number of national regulations. Typically, the CERT follows regulations in their own country, and transfers responsibility to the CERT in the other country to follow regulations on reporting incidents to their local authorities.

The NIS directive [14] was mentioned by several informants as an important contribution to improved reporting and handling of cybersecurity incidents, including incidents related to OT systems. In particular, the NIS Directive gives specific requirements for establishment of incident response procedures for organisations deemed to be part of critical infrastructure. As a curiosity, it can be noted that the Norwegian oil & gas industry is *not* considered part of Norwegian critical infrastructure, but Norwegian natural gas supply *is* considered part of German critical infrastructure.

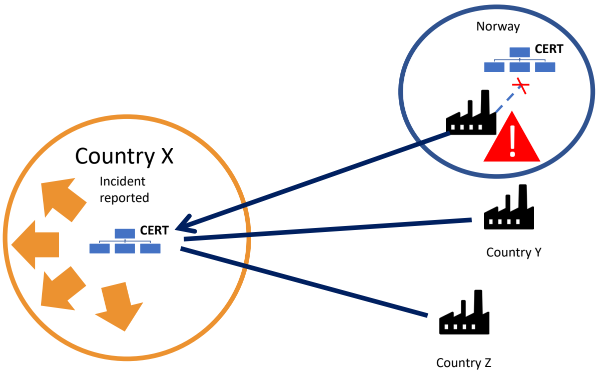

Fig. 1. Imperfect information sharing across borders

B. Monitoring of Cybersecurity Incidents

1) Intrusion Detection System (IDS) sensors: Intrusion detection System (IDS) sensors are largely used for monitoring IT systems, but are not in widespread use for monitoring of OT systems within the oil and gas sector. A CERT informant states that they initiated a pilot project in 2016 where they have deployed sensors that collect information about which systems are used within the OT networks, so that the CERT can send out tailored alerts about vulnerabilities in these systems.

CERTs find that they have more visibility into IT security events than OT incidents, since OT systems often lack network monitoring and intrusion detection solutions. The informants believe that the lack of visibility also applies to CERTs' customers and Safety and Automation System (SAS) suppliers. CERTs find that lack of technical information on OT systems is a challenge when monitoring for cybersecurity incidents. For example, it is difficult for CERTs to get overview over and details about which communication protocols are used, and how ”normal” baseline network traffic looks like on the OT network.

2) Reporting of Cybersecurity Incidents: Several informants point out the difference in reporting and monitoring cybersecurity incidents regarding IT and OT systems.

For cybersecurity incidents, the CERT is dependent on good communication with the company where the incident occurs. The CERT also needs to have pre-established contact with the SAS supplier. This is perceived as helpful, as it allows for better cooperation and contact with both customers and SAS provider, as well as increased capacity for the CERT to convey and influence cybersecurity. Here, the personal contacts with the supplier play an important role. However, handling of cybersecurity related events is not usually part of SAS delivery.

CERTs desire more cooperation with vendors in the incident handling containment phase. Emergency security software

[5] KraftCERT is the Norwegian energy sector CERT, but also caters to other related areas, such as water and wastewater management. See https://www.kraftcert.no for more information.

patching is mentioned as something that can be a particular challenge on machines running OT applications, due to hard real-time requirements of SAS and Safety Instrumented System (SIS) [15] components. Due to safety regulations, the offshore process equipment must be shut down if the SIS is unavailable, and shutdown of an offshore installation implies tens of thousands of dollars in lost revenue per hour.

3) Communication between IT and OT environment: Communication between IT and OT environment is perceived as difficult due to different cultures [16]. Vocabulary used in IT is different than that used in OT, which can lead to misunderstanding and frustration. An example was given where IT personnel almost created a major security incident on the OT side due to a misunderstanding between IT and OT personnel.

A challenge could be that IT professionals become unnecessarily involved in operational issues. An informant refers to a case where they believed they had experienced a security breach, and initiated a major investigation, before realizing that this was only an operations problem. What they thought was suspicious activity on the network was the results of their own activity in connection with incident management. However, it was also pointed out that more collaboration between the IT and OT environments is key to improving the handling of cybersecurity incidents, so it is important not to prevent cooperation by using a too restrictive and detailed definition of OT security breaches.

Some actors have found what they believe is a good balance of maintaining a formal IT/OT separation in respect of the authorities, and professional cooperation on technical problem solving. It is maintained that although there are differences, and it can be challenging to work across IT and OT, it is important to see OT and IT in context.

4) Definition of Cybersecurity Incidents: There are different perceptions among CERTs regarding what is defined as cybersecurity breaches in OT systems. Some informants have no clear definitions of cybersecurity breaches, and they evaluate each incident individually. Some CERTs indicated that their definition of security breaches meant that only targeted intentional actions imply security breaches. That is, they do not include events that are caused by system failures. Other CERTs look at IT and OT systems in an integrated fashion, without emphasizing the distinction between IT and OT security breaches.

Work is underway in some CERTs to create a matrix that defines what is a cybersecurity breach in OT systems.

C. Security Exercises

Security exercises are an important part of preparedness (see ISO/IEC 27035 [7], NIST SP 800-61 [12] and IEC 62443-2-1 [11] 4.3.4.5.1-4 and 4.3.4.5.11). CERTs believe that security exercises are important. In particular, communication has a great focus in a security exercise. Some practise most on how information is communicated, and others on who will be given information. Some CERTs organise security exercises several times a year. Most CERTs focus on big, serious incidents in their drills.

CERTs participate to a varying extent in OT security exercises, and some CERTs say that they do not participate in OT security exercises. Good scenarios should be developed that will expose the effects of IT events in OT systems, but this is perceived as a daunting task. In a CERT environment outside Norway, work is underway to prepare such exercises.

Some CERTs participate annually in national exercises that focus on OT. Since private actors do not necessarily have resources for larger exercises, and rather focus on smaller exercises such as phishing exercises, CERTs want to take part in national exercises organised by the authorities in a greater extent. It is agreed that there is great benefit from participating in national as well as international security exercises, because they provide better cooperation between CERTs and improved understanding of different attack techniques and domain knowledge.

D. Detection and Handling of Security Breaches

Detection and handling of security breaches are described in several standards (see ISO/IEC 27035 [7], NIST SP 800-61 [12] and IEC 62443-2-1 4.3.4.5.5-7 [11]).

Detection of OT security events may occur accidentally or through monitoring. Several informants see considerable value of monitoring in terms of maintaining operational ability.

Proprietary protocols and equipment that suppliers want to keep secret can be a challenge and limit information sharing required for visibility into the systems. Insufficient information on protocols complicates incident handling for a CERT, and requires advanced ”reverse engineering” to create intrusion detection systems. A CERT mentions that each time they add an IDS sensor, they detect strange traffic patterns that are not malicious, but are caused by configuration errors and abandoned systems that were not known to be connected to the network. Often, operational personnel will detect and notify the CERT about incidents, something the CERT depends on. Automatic monitoring will initially be cost effective, but personnel who know the systems well are still an important source of detecting anomalies.

A lack of logging is mentioned by several CERTs as a reason for less attention to incidents in OT than in IT. In large enterprises, it takes time to build infrastructure for logging and monitoring all systems. Several cybersecurity providers offer monitoring of OT networks as a service, but an informant is sceptical about this and believes that this is too risky and can break OT systems. Sometimes CERTs experience that they offer help, but that the customer rather wants to handle the situation themselves.

Many of the CERTS do not want to provide detailed examples of cybersecurity breaches and their handling, but mention that the use of a USB memory stick, often in connection with the provider connecting to their own equipment when they do maintenance, as a common way that malware had entered the OT systems. Cyber attacks by state actors are often highlighted as a major threat, but lack of physical security and access control can be just as important. Availability and integrity may as well be threatened by a USB stick brought in by a vendor performing maintenance and installing software updates to the systems.

In general it is argued that OT systems are well separated from each other, and that it is difficult to traverse a network from IT to OT, not least because of network ”airgapping” which is standard practice in many OT systems. Airgapping means that networks and systems are segregated and physically isolated from each other. This means that viruses cannot easily reach a network from another. However, the airgap can be an illusion if firewalls are misconfigured. If personnel or a vendor are using removable media such as USB memory sticks, it is still possible to spread a malware infection even when the airgap is properly configured using network diodes or similar equipment. Immediate incident handling can include turning off the machine, isolating it, removing the network connection, etc., and then contacting the vendor. Conversely, some security breaches can spread too quickly to turn off machines when the network is large, or if the malware is of the type of a computer worm that spreads without user interaction.

Experience with past events, as well as good plans are important for efficient management of security breaches [6]. Experience causes personnel to know what should be done and have good instincts on how to react in such a situation.

One of the CERT informants recounted an incident in which a malware was detected in an OT system in the power industry. An HMI system ran an outdated Windows XP operating system with administrator user. The company had luckily posed some vulnerability requirements to the SAS provider associated with a specific machine, which prevented the virus from spreading further from the HMI to the process control system. The malware caused increased network activity and this was quickly discovered by the CERT that was monitoring the network. The CERT notified the customer’s IT department about the incident and gave advice on responses to the customer, but no other actors were notified. The customer was given the responsibility to report the incident further.

E. Special Challenges

CERTs consider low awareness of cybersecurity in companies’ governance and management as a challenge, and this can lead to a lack of necessary resources for the improvement and development of cybersecurity. Since security work is not noticed when things are done right, only when something goes wrong, the security work is less visible at the board level. Major security incidents occur so rarely that top management is not always aware of the importance of protecting OT systems against cybersecurity threats. An example of a possible solution is that the CERT organizes OT-focused meetings inviting information security executives (e.g., the Chief Information Security Officer (CISO)), with the aim of facilitating better interaction between management and technicians.

The need for collection of data for visibility and incident management is often overlooked. There is a general lack of logging, and in particular lack of knowing what to log. The organizations are often unaware of what information the police might need in a forensics investigation, and what extent of logging is needed to find the root cause of security incidents. To provide a better understanding, a CERT has asked the police to join ISACs, which would increase the understanding of the necessary forensic data collection. The balance between surveillance and privacy is another challenge, and many organizations are looking for advice on how to be in compliance with privacy regulations such as GDPR, and at the same time collect and process enough data to secure their response readiness for cybersecurity incidents.

It is important that companies know which critical assets in their own organization require protection. Each organization is special and should have different customizations. When the CERT publishes fact sheets with recommendations and suggestions on the use of IEC 62443 standards [11] and NIST guidelines [12], they also encourage company-specific customizations.

Informants said that collaboration on cybersecurity incidents between sectors is useful, but have experienced that it takes time to build up such a collaboration. Internationally, we found one example of close cooperation between sector CERTs by having the NCSC aggregate multiple sector CERTs under one department. The intention is to contribute to increased experience sharing regarding the handling of cybersecurity incidents and how an event in a sector can affect other sectors. In our interview study we also registered one example of an international CERT where IT and OT incidents are handled within the same department.

IV. Conclusions and Recommendations

The informants are relatively satisfied with their own CERT capacity today, but it is acknowledged that one can always improve, for example, in visibility, and real-time monitoring of cybersecurity in OT systems. The national petroleum cybersecurity community seems to be a small but tight environment where the actors have good knowledge of each other. Oil and gas companies and drilling companies share information and experience in various (virtual) meeting places and forums organized by external actors (ISACs). There seems to be greater interest in membership of a sectorial ISAC than a CERT. There is little focus, especially among the smaller companies, on systematic sharing of information and experiences about cybersecurity incidents with each other.

Not all oil and gas companies or drilling rig operators distinguish between cybersecurity incidents in IT and OT systems, and views vary widely concerning who is responsible for security in and between IT and OT. To the extent that a distinction is made, it is often about e.g. reasons for turning off systems to install software updates, and the demanding balance between operational availability and cybersecurity in industrial control systems.

The national and international perception of response readiness is varied and does not provide clear recommendations for organization of sector CERTs. CERT actors pointed out that the number of CERTs must be in proportion to actual access to expertise and resources. Furthermore, there is a need for better communication between CERT actors and key persons within the petroleum industry companies.

Even though CERT functions are largely formalized, personal networks are still very important for information sharing, especially when it comes to exchanging sensitive information. There is a tendency for international CERTs to recognize the difference between cybersecurity of IT and OT, to address the gap, as well as reconcile the approaches. There is a strong need for coordinating and harmonizing cybersecurity in IT and OT systems, as there are significant differences in terminology, maturity of technical solutions, and culture today.

Acknowledgment

This study was funded by the Norwegian Petroleum Safety Authority (PSA) in 2018. Thanks to the participating companies and PSA employees who have provided important input to the study.

References

[1] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer, "Attackers deploy new ICS attack framework TRITON and cause operational disruption to critical infrastructure," Fireeye, 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[2] R. M. Lee, "Trisis," Dragos, 2017. [Online]. Available: https://dragos.com/blog/trisis/

[3] Dragos, "Global oil and gas cyber threat perspective," Dragos, 2019. [Online]. Available: https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf

[4] L. P. Muller, L. Gjesvik, and K. Friis, "Cyber-weapons in international politics; possible sabotage against the norwegian petroleum sector," Norwegian Institute of International Affairs, Tech. Rep. NUPI report 3/2018, 2018. [Online]. Available: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y

[5] H. Orman, "The Morris worm: a fifteen-year perspective," *IEEE Security & Privacy*, vol. 1, no. 5, pp. 35–43, 2003.

[6] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Computers & Security*, vol. 45, pp. 42 – 57, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404814000819

[7] ISO, "Information technology – security techniques – information security incident management – part 1: Principles of incident management," ISO/IEC Standard 27035:2016, 2016. [Online]. Available: https://www.iso.org/standard/75281.html

[8] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, "A Framework for Incident Response Management in the Petroleum Industry," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1–2, pp. 26–37, 2009.

[9] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Current practices and challenges in industrial control organizations regarding information security incident management does size matter? information security incident management in large and small industrial control organizations," *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 12–26, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548215000815

[10] ISO, "Information technology – security techniques – information security management systems – requirements," ISO/IEC Standard 27001:2013, 2013. [Online]. Available: https://www.iso.org/standard/54534.html

[11] IEC, "Information technology – security techniques – information security incident management – part 1: Principles of incident management," IEC Standard 62443-2-1:2010, 2010. [Online]. Available: https://webstore.iec.ch/publication/7030

[12] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," NIST Special Publication 800-61 Revision 2, 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-61r2

[13] PSA, "Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (the management regulations)," Last amended 26 April 2019, Petroleum Safety Authority Norway, 2019. [Online]. Available: https://www.ptil.no/contentassets/f18375b7184d4cd68fc1c733b318b3dc/styringsforskriften_e.pdf

[14] 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. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[15] IEC, "Functional safety – Safety instrumented systems for the process industry sector – part 1: Framework, definitions, system, hardware and application programming requirements," IEC Standard 61511-1:2016 , 2016. [Online]. Available: https://webstore.iec.ch/publication/24241

[16] M. G. Jaatun, M. Bartnes, and I. A. Tøndel, *Zebras and Lions: Better Incident Handling Through Improved Cooperation*. Cham: Springer International Publishing, 2016, pp. 129–139. [Online]. Available: http://jaatun.no/papers/2016/i4cs.pdf