UiA University of Agder

Master

Strengthening incident response efforts in operational technology environments

A qualitative exploratory study exploring the challenges and practices among companies engaged in essential operations

CHRISTOFFER STRAND ARNESEN, HAUK HØEGH KROHN

SUPERVISOR
Devinder Thapa

University of Agder, 2024
Faculty of Social Sciences
Department of Information syste

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

This master thesis represents a culmination of this semester's work and effort. We would therefore like to thank the many people that have contributed through this journey.

We would first like to express our deepest gratitude to our supervision associate Devinder Thapa. Your guidance and support has been invaluable through the whole research process. Your insightful comments and constructive criticism has helped to form this thesis to something we could not have done on our own.

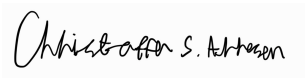
A special thanks will also go to all of our respondents for making this thesis possible. For going out of their way and taking time out of their day to answer our questions, giving us the required empirical data for this thesis. The research would not have been possible without each and everyone of you.

We would also like to show courtesy to our cohabitants, Hedda Fiske-Nygaard og Celine Haslum Andersen. Your friendship and professional discussion have not only been valuable, but also inspiring. We appreciate all the times we have helped each other overcome the challenges and celebrate our success together.

Thank you.

Kristiansand,
June 7th, 2023

Hauk Høegh Krohn



Christoffer Strand Arnesen

Abstract

This master thesis examines the main challenges tied to incident response within operational technology environments, as well as the practices organizations involved in essential operations are implementing to secure a successful approach to incident response in such environments. This is based on our research questions: RQ1: What are the main challenges of Incident Response (IR) within Operational Technology (OT) environments? And RQ2: What practices can organizations engaged in essential operations implement for a successful approach towards IR in OT environments? Based on our findings, we intend to present some practices we think are important to ensure a successful approach to IR in OT environments.

Methodologically, this study has an exploratory qualitative approach. This selection is based on the need to examine incident management in OT environments in their natural context. By gathering data through interviews and previous research and applying an inductive analytical approach, this study gives insight into subjective perceptions and opinions among actors in the OT environment. Through our work, we have focused on the emerging meaning and an evolutionary design where we look for understanding the central principles that are within the field. Our findings from the study show that organizations are facing multiple challenges considering their IR within OT environments, including the handling of legacy systems, the need for continuous operation, the implementation of security updates, and the dependency on third-party vendor support and maintenance. Competence and culture within the organization also play a pivotal role in securing effective IR. Respondents highlight the importance of having robust detection mechanisms and conducting regular exercises and training to improve preparedness.

The implications show that although our findings support existing theory considering the importance of having a solid plan for IR, do they also contribute to new insights that were explicitly not noticed in our systematic literature review. Our study highlights the necessity of dynamic and flexible frameworks for responsibility during incidents, as well as the need for integrated cooperation between IT and OT departments. Other practical implications include recommendations considering the implementation of immutable backups for data integrity, the use of sandboxing, and the development of clear procedures and roles during the IR. The study also underscores the importance of defense-in-depth strategies and diversifying the use of third-party vendors to reduce their vulnerability. To ensure that organizations can have a successful approach to IR within OT environments, they should implement clear procedures for role delegations and decisions, develop risk assessments, secure continuous revision of security procedures, and promote a culture of security awareness and skill development.

Contents

Acknowledgements ii

Abstract iii

List of Figures vii

List of Tables viii

1 Introduction 1
- 1.1 Rationale and motivation . . . 2
- 1.2 Thesis overview . . . 3

2 Background and related work 4
- 2.1 Literature review methodology . . . 4
  - 2.1.1 Objective and research question . . . 4
  - 2.1.2 Inclusion and Exclusion Criteria . . . 5
  - 2.1.3 Search Strategy . . . 5
  - 2.1.4 Screening for inclusion and assessing quality . . . 7
  - 2.1.5 Data extraction . . . 8
  - 2.1.6 Synthesis of Information . . . 8
- 2.2 The Incident Response life cycle . . . 9
  - 2.2.1 Preparation . . . 9
  - 2.2.2 Detection & analysis . . . 10
  - 2.2.3 Containment, eradication & recovery . . . 11
  - 2.2.4 Post-incident activity . . . 12
- 2.3 The challenges of Incident response in OT environments . . . 12
  - 2.3.1 The challenges with OT as a system: . . . 12
  - 2.3.2 Prominent Attack Vectors . . . 15
- 2.4 Responding to cyber incidents in OT environments . . . 17
  - 2.4.1 Preparation and Planning for IR in OT Environments . . . 17
  - 2.4.2 Decision making . . . 19
  - 2.4.3 Responsibilities . . . 21
  - 2.4.4 Detection . . . 23
  - 2.4.5 Recovery after Incidents in OT Environments . . . 24
  - 2.4.6 Post Incident Activity . . . 26

3 Research Approach 29
- 3.1 Qualitative Approach . . . 29
- 3.2 Research Design . . . 30
- 3.3 Data Collection . . . 32
  - 3.3.1 The Interview Process . . . 33
- 3.4 Data Analysis . . . 34
- 3.5 Challenges & Limitations . . . 35

3.6 Ethical Considerations . . . 36

4 Findings **37**
4.1 Organizational Practises . . . 37
4.1.1 Laying the Groundwork: Incident Preparedness . . . 37
4.1.2 Roles and Decisions: Managing the Crisis . . . 40
4.1.3 Early Warning: Detecting Anomalies . . . 42
4.1.4 Resilience in Action: Recovery Strategies . . . 43
4.1.5 Aftermath: Post-Incident Review and Actions . . . 44
4.2 Challenges . . . 45
4.2.1 Legacy Equipment . . . 45
4.2.2 Security Patches and Continuous Uptime . . . 47
4.2.3 Support and Maintenance . . . 48
4.2.4 Culture and Competence . . . 49
4.2.5 Attack Vectors . . . 51

5 Discussions **54**
5.1 Theoretical implications . . . 54
5.2 Practical Implications . . . 59
5.3 Future Work . . . 63
5.4 Limitations . . . 63

6 Conclusion **65**

A Consent Form **67**

B Interview Guide **70**

Bibliography **74**

List of Figures

2.1 Screening for Article inclusion 6
2.2 The Incident Response Life Cycle 9
2.3 Capability Map 18
2.4 ICS Incident Response Framework 20
2.5 Decision Tree 21
2.6 Responsibility Framework 22
2.7 STEP Diagram of Virus Attack 28

3.1 Research Design 31

List of Tables

3.1 Overview of respondents, their positions, and industries 32

Chapter 1

Introduction

As manufacturers embark on the journey of Industry 4.0, marked by heightened digitalization and the infusion of advanced technologies into industrial processes, one critical facet gaining prominence is the concept of convergence between information technology (IT) and operational technology (OT). Historically, IT and OT ecosystems have functioned within distinct and isolated realms, each governing disparate domains. OT, deeply rooted in the physical realm, primarily concerns itself with the management of tangible elements, such as manufacturing systems and industrial equipment. In contrast, IT is entrenched within the digital domain, encompassing areas like servers, network infrastructure, data management, and other digital facets. Consequently, within the organizational framework, IT and OT systems were traditionally regarded as inherently segregated entities (INCIT, 2023).

However, the landscape is evolving rapidly, driven by the imperatives of efficiency, agility, interoperability, socio-economic pressure, and innovation. The advent of interconnected cyber-physical systems and the proliferation of Internet of Things (IoT) devices have blurred the boundaries between IT and OT, accelerating this convergence. This integration is pivotal for achieving smarter, more efficient industrial operations and enhancing overall productivity. This convergence has not only unlocked unparalleled opportunities for synergy and optimization but also introduced new areas of vulnerability. For instance, the IT-OT convergence has resulted in OT environments, such as Industrial Control Systems (ICS), being exposed to a myriad of cyber threats. These threats are exacerbated by the fact that many OT systems were not originally designed with cybersecurity in mind, making them particularly susceptible to attacks. While OT environments are becoming more interconnected and digitally transformed, they are also becoming financially motivated and high-profile targets for threat actors looking to exploit vulnerabilities, disrupt operations, and cause damage on a massive scale. Notable among these cyber threats are a wide range of adversarial tactics, techniques, and procedures, from complex malware and ransomware campaigns to insider exploitation, supply chain insecurity, and newly developed attack vectors (Yassine, 2021).

The Canadian Government's published a report where these new vulnerabilities have engendered intense Canadian federal safety and security and have led to the publication of reports on growing cyber threats to OT, which refer to the system threat landscape. More attacks are growing in terms of complexity and frequency to attack OT; an average of two significant incidents took place during 2010–2019. However, in 2020, 8 and further, report-wise noted as of November 1, 2021 (Canada, 2022). Another relevant piece of data we can mention in this context is the data released by SANS. When asked how the respondents categorize threats against ICS, they rated the threat level as "high," and it was 38 percent in 2019, 41 percent in 2022, and then 44 percent in 2023. This reveals continued threat actors identifying attacks

against ICS as significant, and continued attacks suffer (Parsons, 2023).

The impact of cyber threats targeting ICS/OT ecosystems can be even more disruptive than traditional data breaches and financial losses. Industrial processes are heavily regulated and designed with numerous safety measures in place. As a result, a cybersecurity attack can have disastrous outcomes with regard to safety, security, downtime, and environmental damage. Accordingly, cybersecurity resilience for OT environments is a critical issue for many companies in the critical infrastructure sector. A high level of concern is due to the possible domino effects of an attack: a single compromised system can lead to disruptions in entire production lines or critical services. Therefore, proactive and comprehensive cybersecurity solutions are required. As the landscape has continued to evolve. While IR in IT environments mainly focuses on the confidentiality and integrity of data, in OT environments, it is essential to focus on the availability and integrity of industrial processes and services. Thus, a response to an incident should be well-organized and designed to include multiple facets, such as threat-based assessments and intelligence, detection and containment, forensic investigation, and rapid response. The outline presented shows that the study of the OT-oriented IR plan is justified (Meagher & Dhirani, 2023).

Having delved into the changing landscape of threats, analyzed attack vectors, reviewed existing IR frameworks, and learned from first-hand experiences, the goal of this research is to build a holistic perspective of the challenges and opportunities facing efforts to secure OT from cyber adversaries and articulate practices for the subjects so that damage is minimal. In addition to bridging the gap between theory and practice, this work aspires to provide actionable recommendations that organizations can use to strengthen their OT's security and contribute to survive the challenges against OT-environments.

1.1 Rationale and motivation

During our preliminary research in the previous semester regarding IT/OT convergence in the courses IS-503 and IS-504, we had contact with companies engaged in essential operations that utilize OT in their daily operations. During the work with our pre-study, we were made aware of a problem highlighted by one of our respondents regarding IR in OT. Our respondent mentioned the difficulty of establishing IR plans for OT and highlighted that this is something that many companies that utilize OT struggle with due to its complexity compared to IT. The respondent further mentioned that a lot of companies do not have their IR efforts under control and stated that those that do often don't want to share their knowledge with others. Upon completion of our thesis's pre-study, we looked into the topic of IR in OT and found that this was, to the best of our knowledge, an area that was not widely studied. We also noticed that the information provided online was mostly general guidelines that were often quite vague and could benefit from insights from organizations to tailor them more to the needs of different organizations. Based on this, we aim to contribute to existing theory and practice by exploring the main challenges and existing practices of IR in OT environments by conducting qualitative interviews consisting of seven participating organizations. Through this, we aim to identify common challenges and effective strategies and present some recommendations to ensure a successful approach to IR in OT environments.

1.2 Thesis overview

Chapter 1: Introduction - An overview of the topic, motivation and research goals.

Chapter 2: Background and related work - Presents the previous research on the topic through our literature review.

Chapter 3: Research approach - Presents the chosen research approaches for our study and why they are suitable, including research design, data collection, data analysis, challenges, limitations, and ethical considerations of our study.

Chapter 4: Findings - Presentation of our empirical findings from our interviews.

Chapter 5: Discussion - Here, a detailed discussion of our empirical findings is presented. The findings are discussed in relation to previous research and our research question in the context of both theoretical and practical implications.

Chapter 6: Conclusion - Presents an overview of the most prominent findings and conclusion.

Chapter 2

Background and related work

2.1 Literature review methodology

Literature reviews establish the foundation for academic inquiries and are essential for academic research (Xiao & Watson, 2019). This literature review will analyze the previously published research, articles, and academic work that is relevant to our research question. The review will summarize and synthesize the existing knowledge to establish a clear understanding of what is known within the literature within the field. The studies are derived from our research question and keywords or synonyms related to it. In this chapter, we will provide a detailed rationale for why the studies were chosen for our literature review.

2.1.1 Objective and research question

RQ1: What are the main challenges of Incident Response (IR) within Operational Technology (OT) environments?

RQ2: What practices can organizations engaged in essential operations implement for a successful approach towards IR in OT environments?

The methodology in this literature review is driven by our primary objective, which is to map the main challenges companies involved in essential operations are facing and how they are responding to OT cyber security incidents. When conducting research in the complex domain of incident response within OT, the choice of methodology plays a pivotal role in the quality of our research. The approach to literature review stands out as the optimal choice for our assignments for several reasons. The systematic review consists of getting an overview of existing evidence and knowledge by using pre-specified and standardized methods to identify and critically appraise relevant research on a specific topic, tied to a clearly formulated research question that seeks to answer a specific empirical question such as "To what extent does A contribute to B?". Considering that we want to examine and answer something rather specific, which may be quite complex, a strict and systematic approach is something that we see as the optimal choice to be able to reach our goals for our research.

2.1.2 Inclusion and Exclusion Criteria

Researchers should establish inclusion and exclusion criteria based on the research question(s) when conducting a literature review (Xiao & Watson, 2019).

In this study, we will only include sources that discuss the IR process for OT environments. We may use studies that discuss the IT IR process for comparison purposes, but we will exclude them from this study otherwise. We will mainly seek to include scientific articles, but we will also include articles from trusted sources such as large corporations and/or government agencies if these are relevant to our topic. We will not have any specific age limit for our sources; although IT and cyber security are domains that evolve quite fast, this is not necessarily the case when researching OT. Distributions of OT systems are often very costly, so it is common for these systems to be remain for a longer period.

2.1.3 Search Strategy

Developing a systematic search strategy is important for accessing the most relevant literature. To guide our search strategy, we primarily followed the insights provided by Xiao and Watson (Xiao & Watson, 2019). They emphasize some key aspects, where the first being channels of literature search. They present three primary sources for locating relevant literature: (1) electronic databases, (2) backward searching, and (3) forward searching. Selecting the most appropriate databases and resources is a crucial facet of our search strategy. Because no single database encompasses all published materials, a systematic literature search should include a combination of multiple databases as well as forward and backward search methods. Xiao and Watson underscore the significance of selecting keywords for the search. They advise that "the keywords for the search should be derived from the research question(s)." In our situation, we dissected the main question into key domains, including "OT," "ICS," "IRP," “Incident Response,” and "Cyber Security." We conducted queries in two electronic databases: Web of Science and Scopus. The databases allow for searching in specific fields, such as title, abstract, and keywords. Filtering out a large number of irrelevant results.

The different queries we conducted for our search strategy were:

- “OT AND Incident response plan”
- “OT AND IRP”
- “Operational technology AND IRP”
- “ICS AND Operational technology AND incident response”
- “ICS AND Incident response AND Industrial control system”
- “Industrial control system AND Incident response plan AND cyber”

In the Web of Science database, searching for keywords in the title, abstract, author keywords, and keywords plus fields yielded a total of 24 results using the six different queries. These queries incorporated our key domains and utilized different boolean operators. Our exploration of Scopus produced a total of 63 results using the six different queries. Specifically, the query “OT AND IRP” generated a single result. While the query “ICS AND Incident Response AND Industrial Control System” generated 40 results.

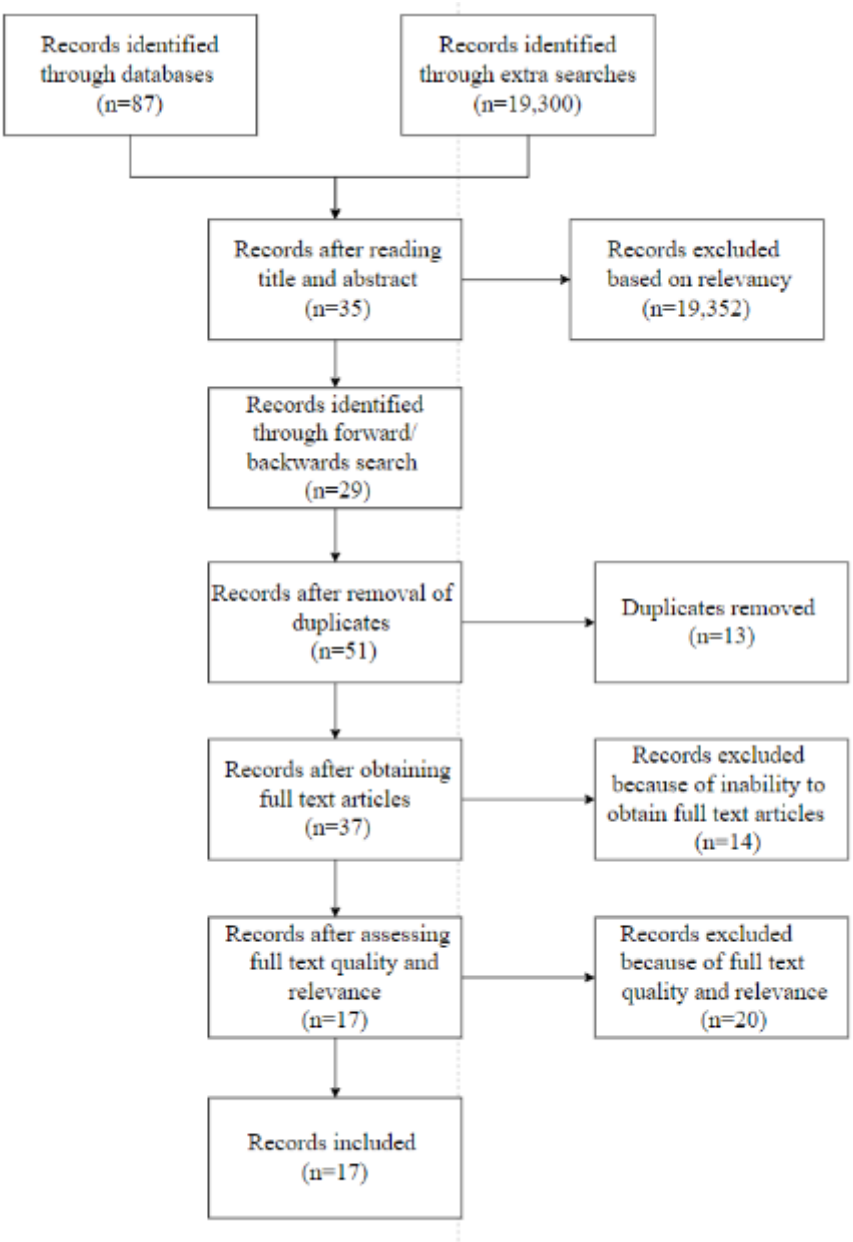


Figure 2.1: Screening for Article inclusion

2.1.4 Screening for inclusion and assessing quality

Researchers should screen each article to be able to decide whether or not it should be included for data extraction and analysis. Xiao and Watson suggest following a two-stage procedure that starts with reading the abstract section of the paper, followed by a refined quality assessment based on a full-text review (Xiao & Watson, 2019).

To determine whether or not a study will be included in our literature review, we have followed their first step, which is reading the abstract chapter for each study's relevance to our research question. As described in our inclusion criteria, we will only seek to include articles that discuss IR in the OT domain. The first step we took to determine each article's relevance was to have a look at the article's title. If the title did not seem to align with our research goal, we saw no point in reading the abstract either. This is because some of the searches returned articles related to other fields of study that were of no relevance to cyber security; it would have been a waste of time to check all of them. Luckily, due to Web of Science and Scopus' ability to search only in the abstract, there were only a small number of hits that did not meet our research goal. If the article's title seemed like something of interest, we read through the abstract, looking for relevance that aligned with our criteria for inclusion and research goals.

Our inquiry into the Web of Science database yielded 24 results across seven distinct search queries. After scrutinizing the abstracts of titles that appeared promising, we identified six articles applicable to our research questions. Subsequently, employing the forward/backward search technique, we discovered an additional 15 relevant articles based on their titles and abstracts. Consequently, our Web of Science database search yielded a total of 21 articles deemed relevant solely through title or abstract analysis.

Exploring Scopus, we retrieved 63 results using the same seven search queries. Employing a similar methodology as with Web of Science, we narrowed down our selection to 27 articles. Further application of the forward and backward search methods augmented our findings with 14 additional relevant articles. Thus, our Scopus search produced a collection of 41 seemingly pertinent articles.

Initially content with the discovery of 62 potentially relevant articles, we endeavored to expand our scope by exploring Google Scholar. Employing the same queries as before, we retrieved an overwhelming total of 19,299 hits. Due to the volume of results, we resorted to sorting some of them by relevance. In doing so, we uncovered one article pertinent to our research, including statistics on cyber threats within the domain of OT. After some time, we realized that we needed some extra literature on the IR process and the lifecycle itself. To find this, we searched on Google and found a guide by NIST that we decided to include.

To determine each paper's quality, we followed Xiao and Watson's second step (Xiao & Watson, 2019). Firstly, we obtained full-text articles and later read through them to evaluate their quality based on the criteria we specified earlier. Initially, getting access to full-text copies of the articles was a problem for some of the articles we found. There were some that we had to pay to get access to, and these were then excluded from our study.

In the first step of the screening process, we encountered a total of 64 potential articles. After conducting a full-text review of each of the 64 articles, we narrowed down our selection to 17 articles we deemed relevant for our literature review. Some of the eliminated articles were duplicates, excessively technical and detailed, behind paywalls, or simply not applicable or relevant to our research.

2.1.5 Data extraction

The choice of a literature review typology and the type of literature synthesized, guide the selection of suitable synthesis methods, which influence the data extraction process. Coding is a crucial step in the data extraction process, especially for extensive reviews. Researchers must decide whether the coding process will be inductive and emerge from the data or deductive and based on preexisting concepts. To ensure consistency and accuracy, it is recommended that researchers code papers together initially to make sure that everyone is on the same page. Xiao and Watson emphasize that it is preferred that at least two researchers code the studies independently. They also emphasize the importance of reviewing the entire paper, not just the results or main interpretation; this is essential to provide context and prevent distortion of the original content. Properly designed forms or codebooks can increase efficiency and reduce errors in the process of coding (Xiao & Watson, 2019).

In this literature review, we will use a hybrid coding approach by combining the deductive coding process and the inductive coding process. We specified some coding subtopics beforehand; this is because we knew that we had to cover certain topics, and it helped us get started. The subtopics that we specified beforehand were the IR lifecycle and the differences between IR in IT and OT. For the rest of the coding, we had the subtopics emerge from the data within two categories; challenges within IR in OT and how organizations should respond to OT cyber incidents. The data extraction process was performed by collecting all the data found in each article, categorized by code, to keep track of information related to the different subtopics we have specified. To start off, both researchers reviewed articles together. This was to make sure that both were in agreement on what information we were to extract from the article. After this, we split up the work and began reviewing articles individually to make the process more effective.

2.1.6 Synthesis of Information

In this literature review, we will address a research question that encompasses cybersecurity challenges related to IR in OT environments. In the process of data extraction, we have divided the research question into two superior topics with each of their own subtopics. Consequently, our approach will involve categorizing the findings into different themes based on whether they represent challenges or how companies should respond. The chosen sources will undergo a comprehensive analysis, wherein we will examine the data extracted from each source. Through this examination, we aim to recognize commonalities and patterns among the data. By identifying these recurring themes and factors, we can gain a deeper understanding of the principal elements that play an important role considering the process of IR within OT, allowing us to pinpoint the key contributors associated with IR in OT and explore solutions for responding to incidents most effectively.

Xiao and Watson emphasize that once the process of data extraction is completed, the reviewer will organize the data according to the review they have chosen. This is often presented as some combination of forms, charts, tables, and a textual description. Upon conducting a thorough analysis and synthesis of the data, our objective is to craft a presentation that enables us to intuitively recognize the factors that contribute the most to the difficulty in the process of IR in OT as well as the practices on how to respond to these incidents. To achieve this we will structure the findings in a clear and concise way, where we first present the IR life cycle, followed by the challenges and the best practices of IR within OT (Xiao & Watson, 2019).

2.2 The Incident Response life cycle

The traditional IR process has four different phases: 1. preparation; 2. detection and analysis; 3. conservation, eradication, and recovery; and 4. post-incident activity. The preparation phase includes forming and training an IR team as well as securing the necessary tools and resources. The preparation phase also includes preemptive measures to minimize incidents by implementing control measures identified through risk analysis. However, there is still a certain degree of risk despite the implementations. This makes the detection of security breaches crucial for alerts, considering an incident. Subsequently, the organization must mitigate and contain the incident based on the incident severity. Through the detection and analysis phase, there is a continuous loop for checking for malware infections while handling existing ones. When an incident is effectively handled should the organization generate a comprehensive report. The report should describe the cause, impact, and preventive measures for future incidents (Cichonski et al., 2012).

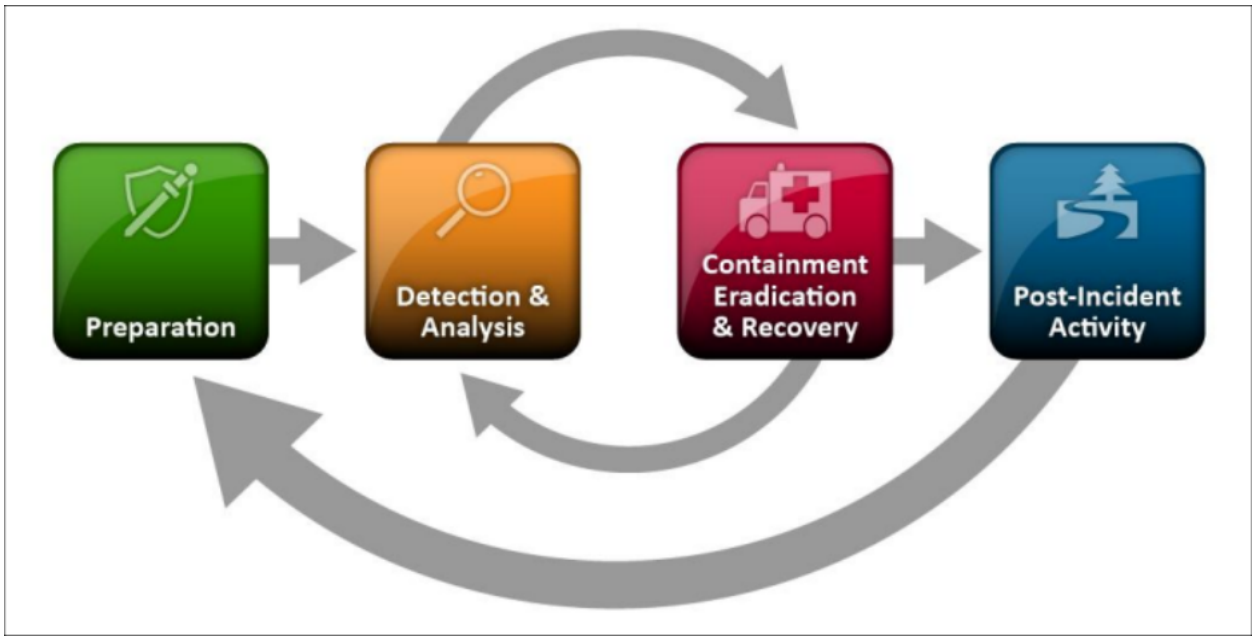


Figure 2.2: The Incident Response Life Cycle

2.2.1 Preparation

IR methodologies commonly include preparation, focusing not only on establishing a robust IR capability to swiftly address incidents, but also on proactively preventing them, to ensure the security of systems, networks and applications. While the IR team's primary role is not to prevent incidents from happening, incident prevention plays a vital role in ensuring the overall success of the IR initiatives (Cichonski et al., 2012).

NIST's guide to computer security incident handling highlights several tools and resources that may be of value during incident handling: Incident handle communications and facilities such as contact information (other IR teams, law enforcement, etc.) and smartphones (to be carried by team members for off-hour support and onsite communications). Incident analysis hardware and software, such as removable media with trusted versions of programs (to be used to gather evidence from systems) and digital forensics workstations (to create disk images, preserve log files, and save other relevant incident data), incident analysis

resources such as port lists, documentation for operating systems, applications, etc., and current baselines of expected network, system, and application activity. Incident mitigation software, such as access to images of clean operating systems and application installations for restoration and recovery purposes, many IR teams create a jump kit; this is a portable case that contains items that could be needed during an investigation. These items could be many of those that were previously mentioned, and the team should avoid borrowing items from this jump kit to make sure that it is available and ready to go at all times. Each incident handler should have a minimum of two computers, one for tasks such as packet sniffing and malware analysis. This laptop may use different software than the rest of the enterprise and should be thoroughly cleaned up and reinstalled after an investigation. The other laptop should be a standard laptop that is used for writing reports and communications (Cichonski et al., 2012).

NIST's guide also states that keeping the number of incidents as low as possible is very important to protect the business processes of the organization. Inadequate security controls may result in an influx of incidents, which may overwhelm the IR team and lead to sluggish and incomplete responses, amplifying the negative business impact such as prolonged periods of service and data unavailability. To keep the number of incidents as low as possible is it important to evaluate and review the potential vulnerabilities that can occur, through risk assessment, and provide mitigation measurements for each of them (Cichonski et al., 2012).

2.2.2 Detection & analysis

Incidents can manifest in numerous forms, making it impractical to devise step-by-step instructions for handling each and every possible scenario. Instead of this approach, organizations should maintain a general preparedness to address any incident, with a focus on being ready to handle events that utilize common attack vectors. NIST lists common attack vectors in their guide. They lists removable media like USB flash drives, web attacks like cross-site scripting attacks, and email message attacks as possible attack vectors. Detecting these incidents and assessing potential incidents accurately is often the most challenging aspect of the IR process for many organizations (Cichonski et al., 2012). NIST highlights three different reasons for this in their guide, the first being the diversity in detection methods such as IDS and manual reporting. Another factor that makes this difficult is the high volume of potential signs. Organizations frequently encounter a significant volume of potential indicators of incidents. The IDS may generate everything from thousands to millions of alerts a day, requiring substantial resources and efforts to go through. The last factor highlighted in NIST's report is specialized technical expertise. Understanding the various attack methods and system behaviors is crucial to being able to properly analyze incident-related data, with a requirement of deep technical knowledge and extensive experience (Cichonski et al., 2012).

The detection and analysis of incidents presents challenges due to potential indicator inaccuracies and the sheer volume of signals received on a daily basis. Even accurate indicators may not always confirm a cyber incident; they may also stem from other causes, including human error. Hence, determining whether the cause stems from a cyber incident requires technical expertise. While some incidents, like a defaced web page, are easily recognizable, many manifest through subtle changes or incomplete symptoms, demanding meticulous analysis. Detecting incidents is particularly challenging, requiring skilled personnel to interpret signals effectively. Technical solutions can help, but they are currently no substitute for a proficient team. A well-trained IR team is essential for efficient handling. They must swiftly validate incidents, conduct initial analysis to ascertain scope and potential impact, and prioritize subsequent actions like containment and deeper investigation (Cichonski et al., 2012).

Determining the priority of incident handling should not solely rely on the availability of resources. Instead, prioritization should consider key factors such as: functional impact and how the incident affects the functionality of IT systems and its impact on users; information impact, like how the incident affects the confidentiality, integrity, and availability of organizational information and recoverability; and how feasible it is to recover from the incident, considering its scale and the resources required. The functional and information impacts in combination determine the overall business impact of the incident. Recoverability guides the team's response. Incidents with high functional impact and low recovery effort warrant immediate action. However, complex incidents may require strategic-level responses, such as involving specialized teams for prevention strategies. Prioritizing responses based on estimated business impact and recovery efforts ensures effective incident management. Organizations can rate incidents using functional impact categories to aid in resource allocation and prioritization (Cichonski et al., 2012).

2.2.3 Containment, eradication & recovery

Another important phase in incident handling is containment. It is necessary to contain the incident to avoid all risks of resource utilization and complicating damage. Early containment ensures the possibility of an adaptive response. Existing strategies and plans make containment decisions easier, such as shutting down systems or disconnecting the network. An organization should define the acceptable risk level and create containment strategies. Containment strategies depend on the type of incident and have published criteria based on which containment decisions are made. Examples of such criteria are potential resource damage, evidence, system or service availability, the time and other resources required for implementation, effectiveness, and duration of the solution. Some attacks may cause additional damage when contained; for instance, disconnecting from a compromised host may trigger malicious processes to escalate damage, such as data encryption. Therefore, we are not guaranteed prevention of further damage by simply disconnecting from the compromised host, and incident handlers should be cautious (Cichonski et al., 2012).

Although the main reason for obtaining evidence in an incident is to prosecute and solve the incident, some legal implications recommend that evidence preservation in a catastrophe should be clearly documented. Additionally, all the processes involved in evidence collection shall be regulated and formulated by legal guidelines established in coordination with the legal administrations and law enforcement jurisdictions to guarantee admissibility in court. Furthermore, evidence handling shall be clearly documented by providing relevant information such as the identifier for the computing resources, the person who collected them, the timestamp at the time of collection, and the storage location. Taking evidence from the computing resource is more complicated since a snapshot of the system may not be available upon detecting the catastrophe. Early acquisition helps preserve the system's state before unintentional alterations occur during investigation. Users and system administrators should be informed about preserving evidence (Cichonski et al., 2012).

After an incident has been contained, eradication becomes an essential part of eliminating all components involved, such as removing malware and deactivating compromised user accounts. The eradication phase also involves ensuring a comprehensive restoration of the affected hosts within the organization to eliminate the exploitation of the vulnerabilities that occurred during the incident. Despite not being required in all incidents, eradication is often integrated into the recovery process. The recovery phase entails restoring the systems to normal operation by reconfiguring the network, ensuring stability, and fully remediating the vulnerabilities that could invite a related incident in the future. Recovery activities may

involve restoring systems from clean backups, processing system reinstallation, replacing replaced or compromised files, applying patches, changing passwords, and improving network security, among other measures. The eradication and recovery efforts should be methodologically phased to streamline the remediation process. In large-scale incidents, eradication can take months, with the first set of activities implemented in days or weeks to deploy short-term, high-value changes that improve the overall security. Subsequent activities may be focused on long-term and strategic infrastructure changes as well as ongoing security modifications (Cichonski et al., 2012).

2.2.4 Post-incident activity

One of the most important parts of IR is learning and improving, IR teams must adapt to emerging threats, advancements in technology and insights learned from previous incidents. Conducting lessons learned after incidents is crucial for enhancing security measures and improving the incident handling process. These meetings should be held shortly after the incident, all involved parties should review the incident, assess effectiveness, and identify areas for improvement. Smaller incidents may require a limited post-incident analysis, while larger attacks on the other hand may require more comprehensive analysis. The success of these meetings depends on involving the right stakeholders and other teams, setting clear agendas, establishing rules of order and documenting key points and action items. These "lessons learned" meetings can also serve as valuable training material for new team members and to inform updates to the IR policies and procedures. Further post incident activity is creating follow up reports for each incident. These reports include a structured timeline of events and their estimated damage that will serve as a reference for future incidents (Cichonski et al., 2012).

Lessons learned activities are meant to give us useful information from each incident. Over time, this collected incident data serves various purposes. It can justify additional funding for the IR team and inform risk assessment processes, leading to the selection and implementation of additional measures. Organizations that report incidents must ensure that they collect the right information, it is important that the collected data has a purpose, and that they don't store a large amount of useless data, making it harder to navigate and assess later. Useful data that should be collected may include, the number of incidents handled, time per incident, objective assessment and assessment of each incident (Cichonski et al., 2012).

2.3 The challenges of Incident response in OT environments

Within OT is IR highlighted as a critical area filled with unique challenges and considerations. This chapter delves into the multi facet area of OT, where it dissect its challenges and nuances through two central sub chapters: Challenges with OT as a system and Prominent attack vectors.

2.3.1 The challenges with OT as a system:

One of the main concern within IT is the prevention of unauthorized access and leakage of sensitive data. As structured in the known CIA triad, where confidentiality comes first, then

integrity and last availability (Samonas & Coss, 2014). On the contrary is the OT domain shifting its focus to protecting against cyber threats that potentially can lead to shutdowns or accidents. The "flipped CIA triad" is often referenced by ICS security experts. They were designed with the requirement that real-time availability comes first, then the integrity of the telemetry data, and lastly confidentiality (Marali et al., 2019). In this sub chapter we will explore the disparities in IR strategies between OT and IT domains, shedding light on the unique challenges and considerations that OT environments encompass (Kanamaru, 2020; Larkin et al., 2014).

Up-time Requirements:

OT systems can control manufacturing processes, energy production, transportation systems, and other critical infrastructure. If there were disruption to these systems, it could potentially result in substantial financial losses, supply chain disruptions, and delays in delivering products to customers. For industries that work on thin margins and have short production deadlines, short periods of downtime can have a multiplier effect on downstream operations and client satisfaction. The ability to continue operations in OT environments is crucial. Unlike IT systems, which can usually have planned downtime for maintenance and updates, ICS processes need extensive pre-deployment testing to guarantee high availability and reliability. Most IT strategies, such as restarting components, are ineffective in an OT setting due to their negative impact on operational requirements and system reliability (Smith et al., 2021). The strict real-time availability requirements of OT environments make continuous operations a requirement, with minimal or zero tolerance for latency or data loss. With the waning prevalence of conventional redundancy mechanisms, which are always capable of continuous operation, maintaining uptime and reliability has become even more challenging. The need for innovative solutions that strike a balance between operational requirements and cybersecurity requirements is highlighted when the "flipped CIA triad," as mentioned, emphasizes the priority of availability in most OT systems (Carr, 2014).

Patch Management:

Patch management in an ICS can also present a challenge due to the unique characteristics of ICS environments. Always-on system modifications to increase safety and security increase the complexity of validation and will require continuous end-to-end testing. However, if these system changes are too difficult or burdensome to the end-users, they will likely be ignored, thus undermining safety and security. Many ICS components are not connected to the Internet, making it impossible to utilize automated patch deployment methods often utilized in conventional IT systems. When connected, the operation's essential nature typically necessitates carefully planned patch implementation to prevent disruptions as required by standards such as IEC 62443-2-3. The ICS also operates in real-time or near-real-time, meaning even small hitches can harm production or result in severe injury. As a result, maintenance routines must be carefully designed and controlled to protect the performance of vital processes while minimizing disruption. This is a serious challenge considering IR in OT. Due to the risk of downtime and subsequent monetary losses, many OT systems rarely include automated update or patch capabilities, unlike traditional IT operations. Furthermore, applying security patches may unintentionally violate system certifications or compromise operational integrity, making it a delicate balancing act between security and functionality. However, applying security patches can introduce performance degradation, necessitating updates to technical standards for transparent communication between suppliers and users

regarding patch impacts. This potential security violation may stop actors from updating their OT systems and having them run on Windows XP, which is no longer supported (Carr, 2014; Larkin et al., 2014; Ying et al., 2015).

Timeliness and Performance requirements

The timeliness and performance requirements serve to differentiate between IT and OT. Unlike IT, ICSs are subject to tight timeliness constraints, and automation must be real-time to guarantee the myriad operations maintain their rhythm. As systems built on real-time operating systems, ICS prioritizes deterministic responses and reliability over throughput. On the other hand, IT systems are designed to maximize throughput while accepting some level of delay and jitter in response from the system (Larkin et al., 2014).

Physical Considerations

Safety considerations surpass any other domain of concern in OT-environments since failures in security could lead to devastating impacts on life and environmental harm. Since ICS systems are closely tied to safety, any safety system compromise in the name of security becomes unacceptable. For instance, a security protocol that stops a gas refinery pump from shutting down leads to consequential explosions. Ideally, ICS components directly control physical systems with complex interactions with the environment. Due to the direct threat posed by any changes in the operational aspect of ICS systems, the system's physical effects require input from control systems specialists and domain-specific experts. An example is the effect of ICS in a chemical manufacturing facility, where a minor malfunction might result in hazardous spills or pump explosions. Additionally, the physical interaction aspect extends to ICS's indirect interaction with the operational space, where experts need to test performance assumptions independently. Since ICSs are primarily managed by control engineers, they present a high risk of assumption-based planning. Control networks in ICS immediately shut down after any disruption to normal functioning, which imposes a significant risk to operation (Stouffer et al., 2011).

Legacy Equipment

The prolonged life cycle of ICS equipment, often spanning 20 years compared to the 3-5 year cycles in traditional IT networks, poses challenges to cybersecurity and IR efforts. Insecure legacy equipment prevalent across critical infrastructure's ICS deployments compounds these challenges, with limited vendor support and prohibitive replacement costs challenging the situation. ICSs are generally poor at supporting forensics, as field devices find it challenging of data logging and storing data for forensic analysis. Intrinsically, the air gap between IT and OT, enforced to operate on firewalls, has been thoroughly penetrated and demonstrated unreliable in the modern battleground, making it intricate to rely on conventional forensics paradigms. ICSs are poor systems, often with multiple resource constraints that are of low modern IT security . In addition, many legacy systems do not support high-level features like encryption, error logging, and password protection and cannot utilize the high-level IT security resources. The broad-ranging protocols already in place are assuredly not updated with the resources to reconstruct and guarantee current and advanced-security measures (Carr, 2014; Lees et al., 2018; Yau et al., 2019b). ICS are often resource-constrained systems lacking modern IT security capabilities. Legacy systems may lack features such as encryption,

error logging, and password protection, making indiscriminate use of IT security practices disruptive. Furthermore, ICS components may not have the computing resources available to retrofit them with current security capabilities, posing challenges for implementing robust security measures in OT environments (Stouffer et al., 2011).

Support

Support in IT systems allows for diversified styles, while in ICS it may be single-vendor-based because of license agreements. Third-party security solutions may be limited to guaranteeing that the loss of service support is minimized. Moreover, multiple ICS vendors offer specialized support to meet industrial requirements, permitting rapid response and resolution of critical issues. Increased interconnectedness due to the convergence of OT and IT ecosystems has created a large number of entry points to various systems that could be exploited. Additionally, weak network segmentation, an increase in access points through the internet, and trusted vendor connections further expand the risk landscape. Consequently, robust access controls and threat mitigation measures are necessary to protect OT environments from the dangers presented by new threats. Furthermore, for an effective IR strategy, organizations need to comprehend these distinctions and create a strategy that distinguishes between IT and OT environments' requirements. Therefore, more awareness is needed to mitigate risks, boost operational resilience, and effectively protect critical infrastructure and processes (Stouffer et al., 2011).

Increased interconnectedness due to the convergence of OT and Information Communication Technology ecosystems has created a large number of entry points to various systems that could be exploited. Additionally, weak network segmentation, an increase in access points through the internet, and trusted vendor connections further expands the risk landscape. Consequently, robust access controls and threat mitigation measures are necessary to protect OT environments from the dangers presented by new threats. Furthermore, for an effective IR strategy, organizations need to comprehend these distinctions and create a strategy that distinguishes between IT and OT environments' requirements. Therefore, more awareness is needed to mitigate risks, boost operational resilience, and effectively protect critical infrastructure and processes (Larkin et al., 2014).

2.3.2 Prominent Attack Vectors

OT environments, particularly ICS, face a myriad of sophisticated attack types that pose significant risk to critical infrastructure and industrial operations. As history has shown us through incidents like WannaCry and NotPetya, it's becoming increasingly apparent that common malware poses a significant threat in the long term. These risks are only expected to rise due to the widening gaps in safeguarding OT compared to IT. As OT becomes more interconnected with the internet, it inevitably becomes a weak point for cyber threats, just like any other connected system. The reason is that OT components frequently use hardware, software, and communication protocols. Moreover, the development and deployment practices that were used to build such interconnected systems and their communication networks are reused vulnerabilities and exploitations: security incidents and threat syntheses based on past and emerging threat actors' networks security. Using lessons learned from past security breaches and current and emerging threat vectors, this chapter synthesizes existing and emerging threat actors and available attack vectors used for compromising and overrunning ICS systems (Kanamaru, 2020).

One of the most significant threats from malicious software in the OT realm is caused by high-tech and elaborate malware such as Stuxnet, which targets engineering tools, PLCs (Programmable Logic Controller), and SCADA (Supervisory Control And Data Acquisition) systems. These malware breaches enter systems through multiple vectors, such as USB flash drives and network shares, and exploit zero-day opportunities to spread across various systems and compromise target systems. Through firmware tampering and live code injection, attackers seize control programs, modify parameters, and drive abnormal behavior in industrial equipment, with the potential of operational disruptions and equipment damage. A prominent feature in OT security cases is the precision of the compromise of engineering equipment accessible in the compromised environment, most notably PLCs. This malware enters engineering equipment connected to networks and local network connections. It then revokes and rewrites the functionality of various devices' programs and parameters connected to PLCs. The subsequent events lead to the burning or stalling of devices and equipment, the latter of which can persist for several months. More critical is the precise nature of these events, which emphasizes the need for timely identification and intervention. In virtual space, cyber-attacks on ICS are divided into two general categories: "simulation" and "crash." "Simulation" attacks mimic emergency signals and alarms, which mislead the personnel but do not damage the plant. A "crash" attack destroys the boilers, equipment, and towers while maintaining the illusion of normality by suppressing true alarms, increasing the alarm rate. While the simulation assault can be seen as technically feasible, the crash assault requires careful planning, making it all the more difficult to detect and recover from a breach. This international interest in crashing instances highlights the significance and universal concern of these high-profile attacks (Kanamaru, 2020).

Security systems, specifically AV and operating system (OS) patch update mechanisms, emerge as prime targets for malware. The analogy of autoimmune diseases is apt, as an overreliance on defense mechanisms can inadvertently transform the defense system into a threat. Instances of AV false positive detections underscore the risks associated with these systems, necessitating careful internal testing, staged roll-outs, and time-delayed deployments to manage potential errors responsibly (Lees et al., 2018).

Worms designed to propagate to PLC's can present a significant threat to the OT landscape. These malicious entities scan networks, attack PLCs, and replicate themselves on the compromised targets. Attacks exploiting embedded system input/output pin control further demonstrate how adversaries can compromise the integrity and availability of PLC's, with potential difficulties in detection. Countermeasures and protection strategies become crucial in mitigating the risks associated with dynamic code injection (Yau et al., 2019a).

Moreover, attacks on ICS have extended from malware to other breaches, such as advanced persistent threats, supply-chain attacks, spear phishing, SQL injection, distributed denial-of-service social engineering, and man-in-the-middle attacks. Considering the Sobig virus incident, Slammer worm, and targeted assaults against SCADA systems, less sophisticated forms of assault, such as unauthorized intrusion, brute force, and insider breaches, remain a genuine and severe danger. Securing OT environments is not a one-time operation. Organizations must adopt an integrated and intelligent approach to cybersecurity that includes advanced threat identification, people-centered safeguarding efforts, and resilient IR to safeguard critical infrastructure from the persistent and increasing risk from adversaries (Larkin et al., 2014; Yau et al., 2019a).

2.4 Responding to cyber incidents in OT environments

In this chapter we will provide insights into what the literature mentions as the essential strategies and best practices for how organizations should effectively respond to cyber incidents within OT environments. The chapter is divided into the following sub chapters: Preparation and Planning, Decision Making, Responsibilities, Detection, Recovery and Post Incident activity.

2.4.1 Preparation and Planning for IR in OT Environments

In OT environments, IR planning is critical to minimize the effects of intrusions. Various guidelines and methodologies emphasize the importance of thorough planning and preparation to effectively respond to incidents. Through planning and preparation, it will be simpler for everyone within the firm to know how to act in the case of an incident, even if there is the absence of a CISO (Chief Information Security Officer) or other security leaders. The process involves defining procedures to be followed when an intrusion occurs, as outlined in NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. Effective IR planning includes several key components (Stouffer et al., 2011).

Classifying incidents and their impact

IR planning involves the classification of incidents based on their potential impact and formulating appropriate response actions. It is essential to identify and classify various types of incidents within OT environments to ensure a tailored response strategy. These responses may range from minimal intervention to full system shutdown, depending on the severity of the incident and its impact on the ICS system and physical processes. Intrusions can vary in severity, requiring risk analysis to determine the sensitivity of the physical system and appropriate recovery actions. Stakeholder involvement is crucial during the preparation phase, including input from operations, engineering, IT, management, legal, and safety departments. Collaborative planning ensures comprehensive coverage and buy-in from all relevant parties (Stouffer et al., 2011).

Integrating diverse skill sets and agile methodologies

Effective IR teams in OT environments require the integration of diverse skill sets and agile methodologies to adapt to dynamic cyber threats. Cross-functional teams, incorporating expertise from various business elements, enhance knowledge exchange and facilitate contextual assistance during IR. The use of capability maps is a method to assess the team's readiness and identify performance gaps (Smith et al., 2021), as shown in 2.3. Additionally, the deployment of IT security mechanisms, such as firewalls and IDS, can offer protection against common attacks, although challenges exist in securing SCADA systems due to their unique characteristics and vulnerabilities (Larkin et al., 2014).

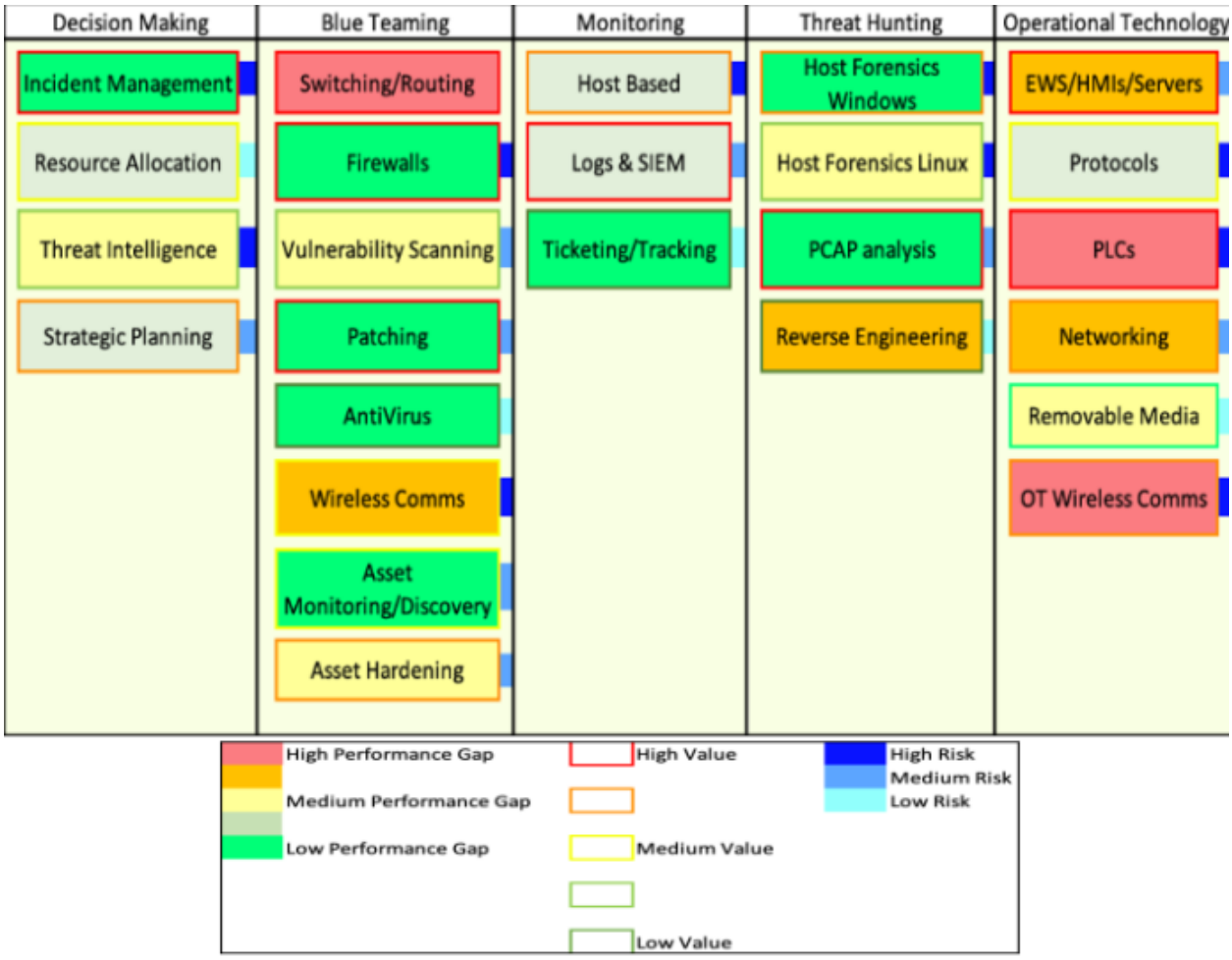


Figure 2.3: Capability Map
(Smith et al., 2021)

Establishing policies and procedures

Investing in the capabilities of outcome avenues drives the organization. To establish a centralized cyber IR team, policies and procedures would be the most important pillars of a response plan. Some of the responsibilities of the team include being an expert resource, sitting on the development of the policies, responding to incidents whenever they arise, and implementing safeguards. The policies account for human resources, information sharing, communication, and the allocation of authorities' responsibilities (Security, 2009). Developing investigative capabilities in OT environments will focus on facilitating integration proofs into existing structures, safeguarding systems and configurations, reviewing key roles and responsibilities, and seeking inter-organizational collaboration (Adrian Pauna, 2013).

Training and Testing

Regular drills and exercises should be mandatory for testing and improving the plan. Organizations may consider some of the inter-organizational response measures at national and international levels. Preparation, conducting, and assessing the outcomes of a demonstrated response may be inconvenient and disruptive. However, it is a risk that is highly unlikely to overburden the business operation. Personnel's availability, reactions and developing roles, sudden decisions, and many human factors are unpredictable. Within a controlled

environment training and testing offers the opportunity for problems that are likely to be experienced in real-life incidents. Conducting such a partial test is productive for assessing unexpected behavior, refining the procedures, and celebrating new team members without somewhat mistakenly incurring full-scale drills. Similarly, IR drills entirely depend on the reproduction of the production system (Security, 2009). Key considerations when setting up IR simulations include:

- Tailoring response levels to different incident types, adjusting scenarios accordingly.
- Simulation worst-case conditions to test preparedness under extreme circumstances.
- Involving all relevant personnel to ensure comprehensive response capabilities.
- Regularly conducting drills to accommodate changes and glean insights from past events.
- Designing scenarios to challenge decision-making processes and uncover potential weaknesses.
- Leveraging external expertise and experiences to enhance drill effectiveness and preparedness (Security, 2009).

Effective preparation and planning for IR in OT environments require an approach encompassing classification of incidents, stakeholder involvement, agile methodologies, capability assessment, team organization, policy development, exercise drills, and collaboration efforts. By integrating these elements, organizations can enhance their readiness to mitigate and respond to cyber threats in OT environments effectively.

2.4.2 Decision making

The framework "An Industrial Control Systems incident response decision framework" proposes three different models for decision making in IR in ICS environments, Descriptive, Predictive and Prescriptive. This models serve as a basis to be able to make better decisions. Descriptive modeling focuses on what has happened or what is happening in this moment. It involves standard signature based detection methods, dynamic incident reporting mechanisms and system logs to document incident details such as time, location and severity. The challenge lies in correlating data from different subsystems to generate descriptive incident knowledge. ICS have unique characteristics compared to IT systems, making traditional detection methods less effective. To address this, they propose the following steps: 1. Capture behaviors or traffic patterns from various detection agents, including distributed agents, adaptors and specialized network probes. 2. Define the profile of descriptive knowledge using formats like the Intrusion Detection message exchange format (IDMEF), detailing the nature and importance of the attack. 3. Correlate information based on the descriptive knowledge profile, aggregating data at the subsystem level to minimize disruption to ICS operations (He et al., 2015).

Predictive modeling's focus lies in anticipating events that will happen in the future and their extent. It utilizes forecasting techniques to identify different patterns and predict the potential spread of the attack. Given the complexity of modern ICS, the challenge is to predict trends from correlated data. The following steps are proposed: 1. Aggregate data from IDS into a correlation engine to generate metadata indicating attack severity and alarm associations. 2. Analyze the aggregated information using a link analysis engine to determine

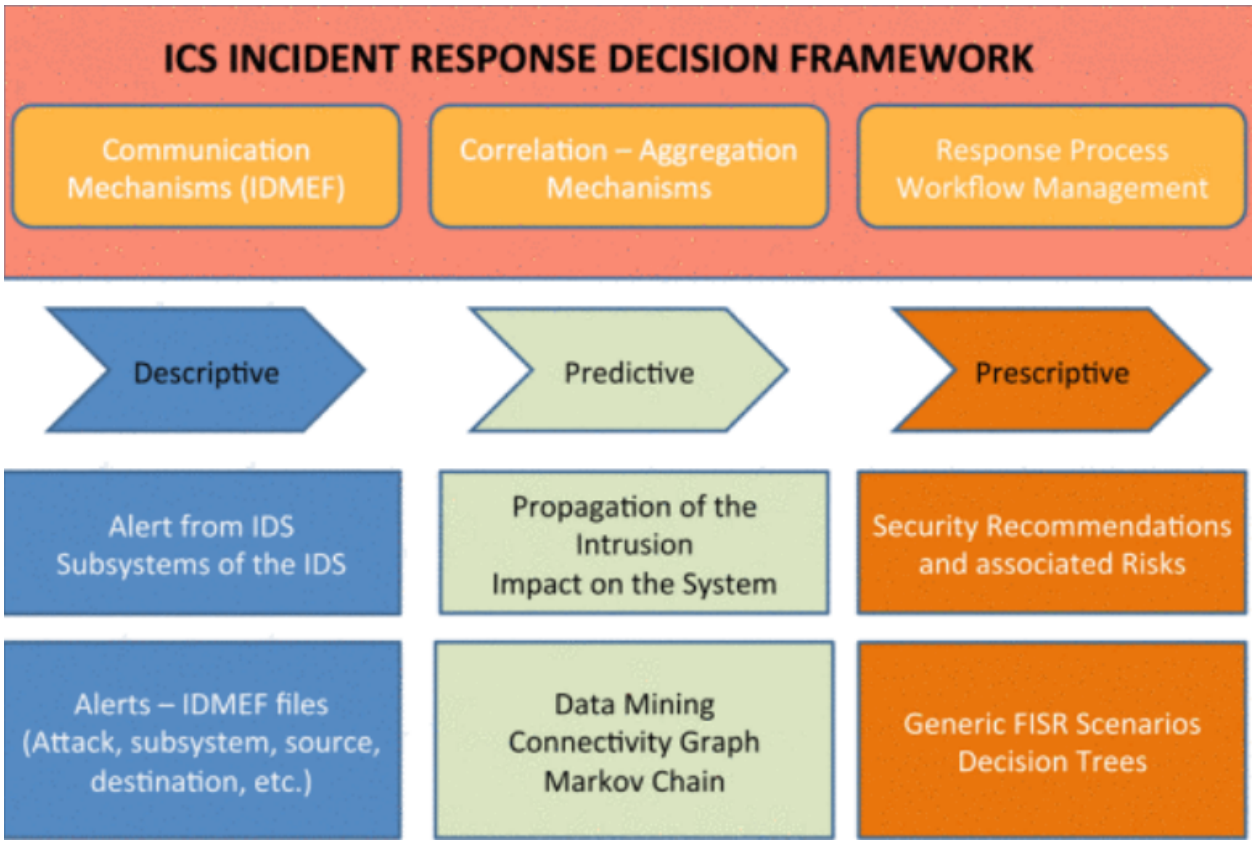


Figure 2.4: ICS Incident Response Framework
(He et al., 2015)

the current system status and vulnerable assets. 3. Use time varying transition processes to correlate interdependencies among subsystems and predict the next system status based on detected attacks (He et al., 2015).

Prescriptive modeling focuses on what actions to take in response to incidents. It combines algorithms and expert knowledge to achieve security objectives, considering the complex dependencies between the ICS components. IR within ICS requires coordination among stakeholders and relies on expert knowledge. The following steps are proposed: 1. Convert ICS expertise into reusable knowledge, detailing procedure based security solutions and associated risks. 2. Define the profile of prescriptive knowledge, detailing procedure-based security solutions and associated risks. 3. Correlate information based on the predefined prescriptive knowledge profile using decision trees to guide IR actions (He et al., 2015).

Another method for taking decisions is using decision trees. The framework "Using Decision Trees to Select Effective Response Strategies in Industrial Control Systems" presents a decision tree framework designed to assist operators in ICS in selecting appropriate response strategies for unwanted events. The framework is based on existing work in the medical and safety fields. To help the operators in this situation, Bayesian network (BN) models have been developed (Chockalingam, 2021).

The decision tree framework begins with identifying the undesired top event, such as a power outage in smart grids. Once this event is first observed, the operator must decide whether to respond or not, and if so, determine whether the event is due to a cyber attack or technical failure. The decision tree structure guides the operator through decisions based on their probability, technical failures and associated causes. By reducing the search space for response strategies, the framework facilitates more informed decision making. Expert

input and probabilistic assessments help determine the most effective response strategy for the specific situation (Chockalingam, 2021).

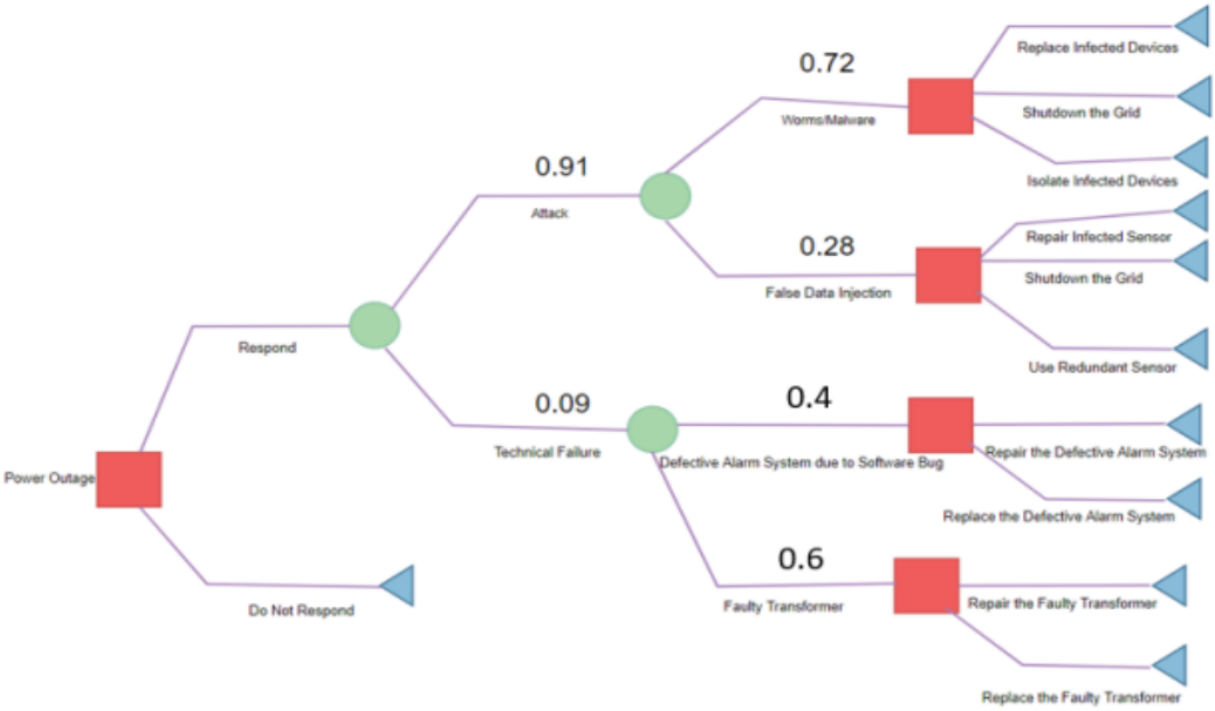


Figure 2.5: Decision Tree
(Chockalingam, 2021)

To demonstrate the framework's application, an example from the energy sector is presented, using probability values from the BN models and established attack vectors, failure causes, and response strategies, a decision tree to guide IR has been constructed. The example above demonstrates how the framework can assist operators in selecting the best possible response strategy based on probabilities and expected values (Chockalingam, 2021).

2.4.3 Responsibilities

In IR, delegation of roles and responsibilities are critical for effective management. Planning, preparation and training fall under the responsibility of the security management. All individuals who identify or suspect an incident must raise an alert to notify relevant personnel. Designated systems or personnel should also be in place to receive alerts, with clear protocols established for reporting incidents in every scenario. Individuals who possess technical system and security expertise should be accessible to support incident recovery either internally or externally. Designated personnel should be tasked with leading the IR efforts, ensuring efficient resolution and recovery processes. Management plays a pivotal role in decision making through the IR process and must be able to make critical decisions at all times. Security management oversees post-incident activities such as analysis, documentation and implementing lessons learned to enhance the response strategies in the future (Jaatun et al., 2009).

A framework developed by students from a Japanese university proposes a dynamic approach to delegation of responsibility. To be able to effectively respond to incidents, the departments

leading the processes must switch dynamically based on the implemented cyber IR step. The responsible departments are the following:

- Operations staff: Recognize abnormal behavior on the plant based on their familiarity with the normal system operations
- ICS-Security IR Team (ICS-CERT): Execute initial responses to ensure plant safety upon detecting abnormalities.
- ICS-Security IR Team (ICS-SIRT): Identify and isolate the affected parts, safeguard the ICS against further attacks and ensure minimal device use for plant operations while collaborating with the management.
- Computer Security Incident Response Team (CSIRT): Address cyber threats in the information system, cooperate with the management and eliminate the risk of future cyberattacks (Hirai et al., 2017).

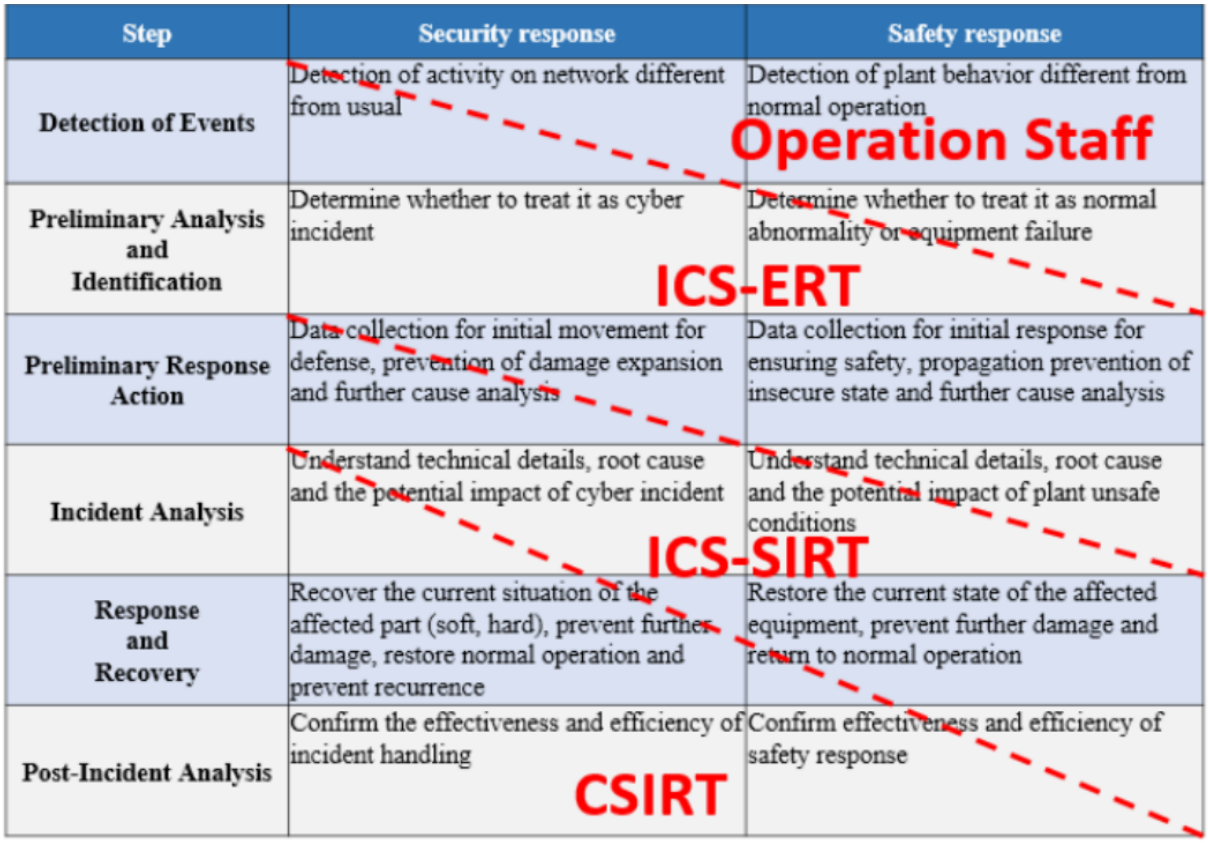


Figure 2.6: Responsibility Framework
(Hirai et al., 2017)

There is also a guide from Homeland Security with recommended practices for developing ICS cybersecurity IR capabilities, these practices provides a more detailed look at the roles. They notice the importance to assign and identify roles to establish a successful IR capability. The following roles are recommended within the Computer security IR team (CSIRT):

- CSIRT team manager: Oversees team organization and objectives, with authority granted by senior management. This person is crucial for assembling resources to handle incidents effectively.

- Process or Control system engineer: This person acts as the expert on the control system architecture and provides insights on normal and abnormal equipment behavior and potential impact on operations.
- Network administrator: This person plays a vital role in responding to incidents involving cyber attacks originating from the network. Offering expertise in network access, security vulnerabilities and system monitoring.
- System administrator: This person manages control system operations and IT administration, with knowledge of access permissions, system logs as well as potential vulnerabilities.
- Plant Manager: This person is Involved in decision-making regarding interrupting operations, risk assessment, funding CSIRT tasks, and coordinating with executive management and external parties.
- IT Director, CIO, or Chief Engineer: Coordinates resources and delegation of authority for IR, given the integration of control systems into existing IT networks.
- Security Experts: Provide cybersecurity expertise, including knowledge of vulnerabilities, exploits, prevention techniques, and incident recovery.
- Legal Experts: Ensure compliance with laws and regulations, assist in evidence collection, and offer guidance on legal issues and privacy rights.
- Human Resources (HR) Specialist: Handles internal incidents, legal issues, policies, and procedures related to personnel.
- Vendor Support Engineers: Offer technical support on equipment and systems involved in incidents, providing valuable expertise in asset restoration and patch creation.
- Other Support Staff: Additional expertise may be added as needed, including legal, law enforcement, forensics specialists, risk management specialists, and administrative support personnel (Security, 2009).

2.4.4 Detection

Information security incidents are usually identified in one of two ways: by coincidence, where someone notices something unusual, or through the routine use of automated technical security measures like IDS or virus scanners. Both of these methods of detection are equally important, which means that the employees must be aware of their responsibility to send alerts whenever irregularities are discovered (Jaatun et al., 2009). Typical warning signs of cyber incidents could be unusual network traffic, disk space limitations, high CPU usage, new user accounts, AV alerts, unexpected patch changes. The operator's experience is valuable for detecting variation from normal behavior (Security, 2009).

The methods for cyber attack detection differ before and after the onset of the malware disturbance. Before the onset the security operations center (SOC) can detect threats like malware using IDS and access log analysis. Suspicious messages are monitored and analyzed to detect unauthorized intrusions. After the malware onset, detection becomes more complex. Operators may notice inconsistencies between system alarms and actual operations. In some cases, cyber attacks are "camouflaged" making detection challenging because the operator does not see anything out of the ordinary through the control system (Kanamaru, 2020).

SCADA systems have unique features and limitations that require specialized security approaches. Traditional security tools like network IDS or AV software may not be suitable due to potential delays or the risk of system failure. Relying completely on pattern-based detection algorithms is no longer enough because of the ever-more sophisticated cyber threats. Instead, security measures must address emerging threats effectively while balancing the ease of maintenance and detection capabilities. Involving a defense-in-depth strategy could layer multiple security controls to minimize risks to protected assets. By adding these extra barriers, the attackers are slowed down, giving the monitoring services extra time to detect and respond to threats. This approach ensures that no single point of failure exists, as different layers of protection are in place to protect assets from various threats (Maglaras et al., 2018).

Every incident must be assessed considering its severity and the following steps to be taken. During assessment, the following actions are taken: Acknowledge receipt of the alert and gather additional information to determine severity, scope, and stakeholders. Notify additional personnel, including experts and suppliers, if necessary. Immediate response is crucial in a process control environment to keep systems running as long as possible. However, a reasonable first action is to isolate the SCADA system by disconnecting it from all external networks. The activation of surveillance systems can help achieve a better understanding of the incident. During an incident, the best decisions are made when the organization has already prepared for the incident types that have the highest likelihood of affecting it and has already defined actions to take in each scenario in advance. In ICS environments, it is especially important to know which actions are applicable to the different types of equipment. In duplicated configurations, the infected units may be disconnected and restored to a known good backup. For other types of equipment, this may not be possible where the removal of a component can trigger shutdowns due to integrated watchdog functions. Incident handlers must try to isolate the infected equipment without disconnecting it or shutting it down. However, health, safety, and environment (HSE) is always the first priority on an offshore installation. If HSE is threatened by continued operations, a shutdown is inevitable (Jaatun et al., 2009).

If an incident escalates and the team does not have the needed expertise, they cannot get the incident under control, the incident is more serious than originally anticipated, or upper management decisions are necessary, the team will require assistance from external parties. Every incident must be documented with respect to what happened, which systems were affected, what damage occurred, and how the incident starts when the alert is raised. False alarms should also be documented. Documentation starts as soon as the alert is raised and continues throughout the response process (Jaatun et al., 2009). The documentation process must be made clear and easy for it to be effective; utilizing a reporting form or template is preferred to make sure that the documentation is structured and that the key aspects are covered. Documenting incidents is key to ensuring that stakeholders are informed, sharing best practices, learning from previous experiences, and conducting post-incident analysis (Security, 2009).

2.4.5 Recovery after Incidents in OT Environments

Recovery after incidents in OT environments is a complex process that requires careful consideration, cooperation, and specialized expertise. Considering post cyber attacks, swift action is required to reduce the impact on ICS. Measurements like partial isolation could prevent further harm if the threat attack is in its early stages. During the partial isolation phase, could it be crucial to consult with operators and maintainers, who can provide direc-

tion on whether a partial or full shutdown is required. Organizations should perform careful preparation on how to recover after the isolation and containment phases, with the ultimate goal being to prevent harm from expanding. In this chapter do we discuss recovery preparation in terms of recovery plans, guided by an analysis of attack techniques and infectivity, to gain a fuller understanding of the threat environment (Jaatun et al., 2009; Kanamaru, 2020).

Recovery requires seamless cooperation among various teams, including SOC, operators, maintainers, and IT staff. The IT/OT collaboration role is crucial for sharing symptomatic events, notifying relevant parties of cyber attack detection, and managing ICS program settings. Effective collaboration between maintainers and operators accelerates recovery procedures. Meanwhile, the SOC is responsible for overseeing the process to ensure adherence to the recovery plan and to address any unintended consequences. When responding to and recovering from OT incidents, forensic investigators must have a deep understanding of SCADA systems and the functioning of embedded devices (Adrian Pauna, 2013; Kanamaru, 2020).

Forensic investigation of OT involves the exploitation of SCADA hardware, software, and firmware, as well as its numerous communications protocols. The lack of logging functions and the volume of low-level data complicate data collection (Adrian Pauna, 2013; Yau et al., 2019a). Existing IR models in SCADA systems lack detailed documentation at a low level, unlike those available for normal IT systems. While guidelines such as Homeland Security's "Developing an Industrial Control Systems Cybersecurity Incident Response Capability" provide general advice, specific forensic incident models for ICS/SCADA are lacking (Yau et al., 2019a).

The environment of ICS presents recovery and restoration challenges that are distinct from reverse processes in a conventional IT context, as previously described. Many of these steps are identical to traditional IT, in particular eliminating viruses, uploading backup data, gradually releasing temporary containment measures, and resetting operational systems and applications. However, incident management in ICS is more complicated, and it introduces even more difficulty, as previously stated, due to the critical nature of the systems used for it. In many cases, it is impractical to discontinue services during the response. ICS needs additional strategies to mitigate, recover, and restore, such as fail-over procedures, temporary or restricted capability backup equipment, or firewalling backup systems from network access. While these measures keep vital equipment and processes running, they operate temporarily with reduced integration and functionality (Security, 2009).

The imperative for continuous operation in this temporary state elevates enterprise risk. Although redundancy in the systems is essential, achieving triple redundancy is often impractical due to cost and complexity constraints. Consequently, if backup systems fail, production halts, placing immense pressure on the CSIRT and operational teams to expedite restoration. For recovery and restoration for ICS does Homeland Security have several recommendations (Security, 2009).

- Establishing contingency plans with available equipment identified before the incident. This will allow operations to continue while primary systems are being restored.
- Patch and maintain all backup systems to the same level as the primary systems.
- Conduct regular and planned testing at a planned specific time to verify that the fail-over systems will work properly when called upon.
- Establish plans to run segments of the ICS in isolation prior to an incident. This

will provide the engineers a realistic picture of interdependencies between components, allowing them to make decisions on isolation, if necessary.

- Test backup equipment against realistic timeframes found in a worst-case scenario. E.g., backup generators may need to power a system for days rather than hours, depending on the circumstances of the facility.
- Establish and rec acceptance tests and procedures to ensure that systems have been restored to the pre-incident state. These may include both automated and manual tests.
- Define procedures as part of the IR plan to provide for the proper authority to accept the test and declare the ICS fully operational (Security, 2009).

Recovering from incidents in OT environments demands a coordinated approach, integrating technical expertise, collaboration, and organizational learning. By leveraging IT/OT cooperation functions, fostering collaboration among stakeholders, and addressing operational challenges, organizations can enhance their resilience against cyber threats and minimize downtime in critical infrastructure systems.

2.4.6 Post Incident Activity

Incident learning is a unique process that supplies new capabilities to modern organizational management systems. Cooke's vision inspires incident learning systems, enabling organizations to gain a fresh perspective on their safety and performance. The carefully examined and considered lessons acquired as a result of incidents then serve as the backbone for organizational resilience.

Cooke defines an incident learning system as an organizational capability enabling the extraction of valuable insights from incidents to enhance organizational performance over time. The learning phase in IRMA (Incident Response and Management Architecture) emphasizes deriving lessons from actual incidents through structured processes and analyses. Cooke describes this system as "the collection of organizational capabilities that enable the organization to extract useful information from incidents of all kinds and to use this information to improve organizational performance over time." For success, it is important that the organization follow the steps, fully commit, and extend resources to facilitate learning from incidents. However, to be able to do so, the learning phase is dependent on the incident's documentation. A structured accident analysis can help identify the causes and cover organizational, technical, and human factors issues. False alarms should also be implemented (Jaatun et al., 2009).

Identifying Sequences of Events using STEP (Jaatun et al., 2009)

- The STEP method facilitates detailed incident and accident analysis through graphical representation. For using STEP:
  - The actors, objects or persons affected by the incident are identified.
  - Events, how they were influenced and how they were handled are placed in a diagram according to the order they occurred.
  - Relationships between the events and what caused them are identified and incorporated in the diagram, linking them with arrows.

Identifying Root Causes and Barriers

- Utilizing STEP diagrams, organizations identify root causes and weak points contributing to incidents. Weak points are analyzed through barrier assessments, which recommend technical, human, or organizational countermeasures. Fig. 2.7 shows four weak points identified

Recommend Security Improvements

- Based on accident analysis and barrier assessment, security recommendations are prioritized using cost-benefit analyses. Responsibility for implementing recommendations is explicitly assigned to ensure effective security enhancement.

Evaluate the Incident Handling process

- The Learn phase encompasses evaluating the incident handling process to identify areas for improvement. Factors considered include the effectiveness of incident management plans, involvement of relevant actors, adequacy of incident detection and recovery procedures, and efficiency of communication throughout the process. Questions to be asked for evaluation could be:
  - Did the incident management plan work as intended?
  - Were all relevant actors involved at the right time?
  - Are there procedures or tools that would have aided incident detection?
  - Are there procedures or tools that would have aided the recovery process?
  - Were the communications about the incident to relevant parties effective throughout the detection and recovery process?

In the modern landscape of organizational management, obtaining and collecting insights from incidents is more than beneficial; it is imperative for building resilience, ensuring security, and enhancing performance overall. Cooke's visionary theory framework envisioned incident learning as a crucial operational capability that organizations use to extract significant knowledge and insights for ongoing improvement.

According to Cooke, the incident learning system is an organizational capability that serves as a conduit for deriving lessons from actual incidents through structured processes and analyses. It encapsulates a set of organizational capabilities that facilitate the extraction of useful information from incidents, thereby nurturing organizational performance over time. However, for organizations to fully realize the potential of incident learning systems, a steadfast commitment to following the prescribed steps and allocating necessary resources is imperative (Jaatun et al., 2009).

Furthermore, most evaluation takes place in the learning phase of the incident handling process because it is critical to enabling an organization to identify areas of weakness that need improvement. Post-incident evaluations, among other things, refine incident management plans, detection and recovery protocols, and communication schemes. Through incident learning systems and a comprehensive process of evaluating and enhancing IR processes, organizations can bolster their resilience, reduce their potential risk, and excel in a changing threat environment. Basically, incident learning systems and post-incident equities assist in setting the overall tone for organizational growth and innovation, allow one to prosper despite difficult situations, and leverage opportunities provided.

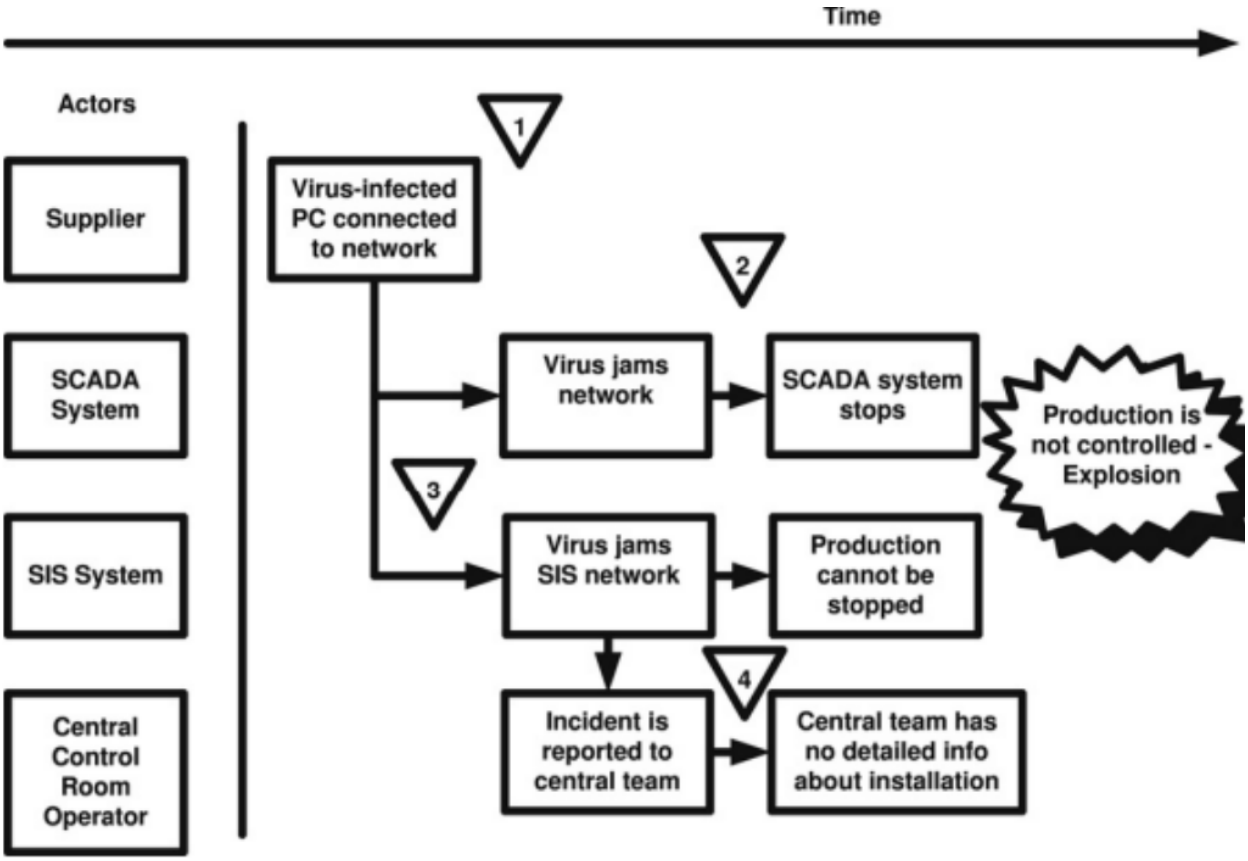


Figure 2.7: STEP Diagram of Virus Attack
(Jaatun et al., 2009)

Chapter 3

Research Approach

Our study's main objective is to come up with recommendations for a successful approach to IR in OT environments. To do this we have to understand and map the challenges as well as the current state of organizational practise regarding organizations approach to IR in OT environments. The study will be guided by the following RQ's:

- *RQ1: What are the main challenges of Incident Response (IR) within Operational Technology (OT) environments*
- *RQ2: What practices can organizations engaged in essential operations implement for a successful approach towards IR in OT environments?*

In this chapter, we will discuss our research approach and the philosophical assumptions we had for the project. We will further explain the methodology for our research design and continue with how we collected our data and analyzed it. Later in the chapter, different limitations and challenges will be highlighted.

3.1 Qualitative Approach

Qualitative strategies are procedures that feature research methods like case study, ethnography, and phenomenology; they also have an emphasis on qualitative data, a focus on words (Recker, 2021).

There are emphasized seven basic and common principles of qualitative methods: (1) natural setting; (2) researchers as a key instrument; (3) multiple sources of data; (4) inductive analysis; (5) focus on emergent meaning; (6) evolutionary design; and (7) holistic and contextual (Recker, 2021). The principles align with our research question, and here's why we find them particularly suited to our study.

- **Natural setting:** Given the complexity and real-world implications of IR in OT environments, studying this phenomenon in its natural setting is crucial. In our case this involves keeping the interviews related to the respondents specific organization and their operations to gain the best possible insights. This approach allows us to understand the context, challenges, and interactions as they occur, which is vital for addressing security concerns effectively.

- **Researchers as a key instrument:** In the context of IR in OT where real-world expertise is valuable, being actively engaged in data collection through methods like interviewing and observation ensures a nuanced understanding of the subject matter.
- **Multiple sources of data:** The multifaceted nature of security challenges related to IR in OT environments demands the collection of diverse data types, such as interviews, documents, and observations. This variety enhances the richness of the research findings. In our case, we have both literature as well as interviews.
- **Inductive analysis:** In light of the dynamic evolution of IR in OT environments and the imperative to address emerging threats and challenges, adopting an inductive analytical approach proves invaluable. This mode of thinking has consistently underscored our entire research methodology, especially considering the inherent subjectivity in our data collection process, among other factors.
- **Focus on emergent meaning:** Understanding the meaning and perceptions of stakeholders in IR in OT environments is fundamental to addressing security and privacy concerns effectively. Qualitative methods excel at uncovering these subjective viewpoints.
- **Evolutionary design:** The ever-changing landscape of OT necessitates a flexible research design that can adapt to new developments and insights. An evolutionary approach aligns with the dynamic nature of the field and promotes research responsiveness.
- **Holistic and contextual:** IR in OT is a complex phenomenon that cannot be reduced to a few variables. Qualitative methods allow us to explore multiple perspectives, providing a comprehensive and contextual understanding that is crucial for developing effective security measures.

3.2 Research Design

A research design serves as a roadmap for gathering, measuring and analyzing data to address a specific research question. It should be cost-effective and reflect intricate planning decisions, which often involve balancing resources, time constraints, data quality, and accessibility. Recker mentions three types of research designs for intellectual reasoning: induction, deduction and abduction (Recker, 2021).

Induction is a technique where you draw general conclusions based on specific observations or data. It entails recognizing patterns to form hypotheses or theories. The strength of inductive arguments can vary; some of them may be weak due to a limited number of observations. While induction doesn't offer any proof, it can be a valuable tool for generating explanations or hypotheses based on educated guesses. Case studies may use inductive reasoning to form theories from observed data (Recker, 2021).

Deduction it is often used to predict a result based on a specific theory or a hypothesis. The main goal of deductive reasoning is to predict outcomes based on a specific theory. Deductive reasoning involves testing different theories up against new data to show potential connections between the theories and the new data (Recker, 2021).

Abduction is another form of reasoning where you make sense of an observation by coming up with the most suitable explanation. Abduction involves a search for new ideas or the-

ories rather than justifying or formally inferring. It's more about discovery or design than validation (Recker, 2021).

The creation of new knowledge in research often requires using a mix of induction, deduction, and abduction, instead of relying on just one method in its entirety. Every one of them comes with its own pros and cons. Induction is useful for generating various theories based on observations but is not able to completely prove them. Testing theories through deduction is possible, but it requires strong foundational theories. Abduction may result in new concepts, but it requires careful observation and understanding of the current guidelines. Observation plays a crucial role in every type of reasoning, aiding in the exploration of phenomena through the identification of systematic patterns. Effective research plans frequently combine exploration, rationalisation, and validation. The progression is not a straight line and frequently circles back and forth, with each stage influencing the others. Exploration lays the groundwork for rationalisation, which may result in additional exploration or validation. Validation requires creating hypotheses that can be tested based on overarching theories, and then putting them through practical experimentation. The results of exploration and reasoning contribute to the validation process, which could lead to more exploration or improvement of outcomes (Recker, 2021).

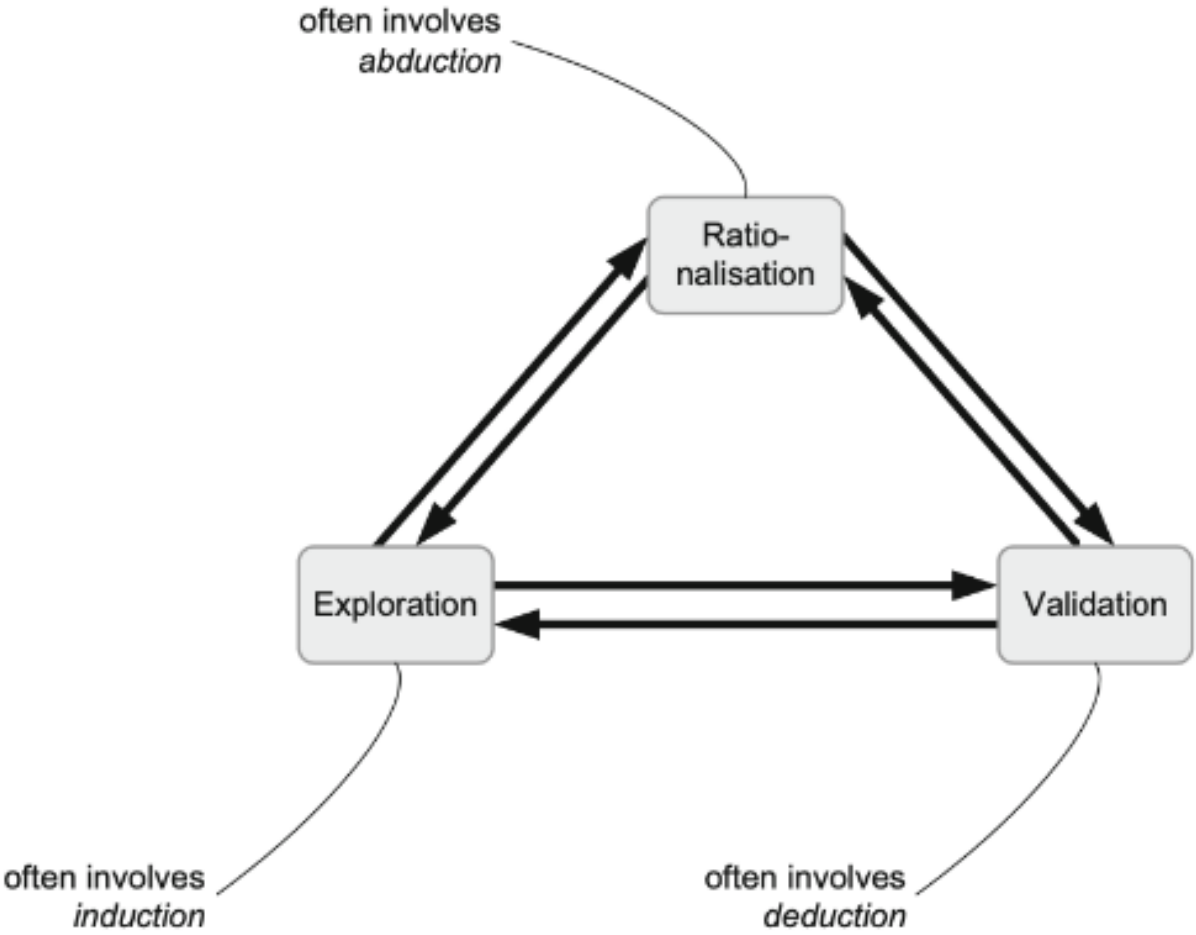


Figure 3.1: Research Design
(Recker, 2021)

Based on Reckers insights, we deem the exploratory category as the most suitable option for our study. The main purpose of our study is to build on existing theory with the contribution of new information from our informants. With the exploratory approach, this will help us in coming up with recommendations based on the findings of our interviews. However, we will also include validation in our study to some degree. This is to see how the literature compares to the current state of OT IR in the real world and see if the literature is confirmed or contradicted.

3.3 Data Collection

Qualitative researchers use a variety of data, such as text, videos, images, sounds, written, spoken, or otherwise communicated accounts for behaviors. This data could be generated from interviews or focus groups; it can naturally occur in observations of regular conversations or in digitally recorded behaviors and communication in online forms, social media, or emails. Interviews is the most common form of qualitative method, which also is our chosen method for data collection (Recker, 2021).

Interviews serve as a way to construct knowledge, typically between the researcher and key informants. These informants hold specialized knowledge in a research setting, providing insights into people, processes, events, or phenomena that surpass the depth, detail, or access available to the ordinary. He further emphasized that these key informants play a crucial role as valuable sources of information in the research (Recker, 2021). In our case, these key informants are people who currently work with cybersecurity in OT. In our search for suitable interview participants, we targeted Norwegian companies that are engaged in essential operations, known to utilize or possess knowledge of cybersecurity in OT. We also ensured that we had representation from various industry sectors. The informants were contacted primarily through email, as well as phone calls when email addresses were unavailable. Ultimately, we successfully recruited seven informants for our study, some information about the informants can be seen in table 3.1 below.

Respondent	**Position**	**Industry**
1	Head of IT	Industry and production
2	Head of IT	Food Production
3	IT Manager	Waste Management
4	Head of Digital Security	Energy
5	Cybersecurity Executive	Oil & Gas
6	Consultant	Cybersecurity Consultation
7	Technical manager	Oil & Gas

Table 3.1: Overview of respondents, their positions, and industries

Respondent 1 has a long experience working with IT in the pharmaceutical industry; one of their main focus areas has been on the industrial and production sides, working with ICS and OT. Their position is now Head of IT in a newly established production company.

Respondent 2 is currently Head of IT at a food production company. They have a long prior experience working as a software architect and IT manager in the financial industry, as well as working as a consultant in consulting firms.

Respondent 3 currently works as an IT manager in waste management. They have prior experience in the oil and gas industry, where they have a lot of experience working with OT.

Respondent 4 currently works as head of digital security in the energy sector, they have a wide experience in working with IT and a long experience working with security within IT and OT.

Respondent 5 currently works as a cybersecurity executive in the oil and gas industry. They have many years of experience working as an IT consultant as well as working with security within OT, among other things.

Respondent 6 currently works in a company that offers services and delivers software to secure critical infrastructure. They have 10-15 years of experience in working with OT, and currently focus on security.

Respondent 7 is currently working as a technical manager for one of their six oil facilities. He has a long experience with UNIX machines and has worked as IT manager.

3.3.1 The Interview Process

There are three different types of interviews: structured, unstructured, and semi-structured interviews. Structured interviews follow pre-planned sets of questions. Unstructured interviews do not follow any predefined plan or sequence, which makes them sort of open-ended conversations. Semi-structured is the most common interview method among the three. These interviews follow protocols where respondents are asked about a topic, and the interviewer can come up with more specific follow-up questions in response to the respondents answer. Semi-structured interviews normally start with general questions that are formulated ahead of the interview and allow for follow-up questions that are typically not pre-formulated (Recker, 2021). For our research, semi-structured interviews seemed like the best fit. This is due to its flexible nature. Although our background research suggests potential challenges, we want respondents to provide their most suitable answers without our interference. This is to make sure that we do what we can to prevent introducing any sort of subjectivity or bias, making the respondent say what they think we want to hear, which can be a challenge to interviews as a method. (Recker, 2021). Topics and questions for the interview could be given out to the respondents in advance so that they can prepare some answers, and that in some cases it is desirable that the informants are surprised with questions (Recker, 2021). We chose to provide the respondents with general questions in advance. Additionally, we have prepared specific follow-up questions, which will be introduced as surprises if the respondents don't naturally address certain factors when responding to the general questions. This approach allows respondents to answer openly without influence. However, it also ensures that we can inquire about specific aspects we are interested in hearing more about if they aren't explicitly mentioned in their initial responses to the general questions.

Our research is split up into two parts: RQ1 seeks to understand the general cybersecurity challenges of IR within OT. RQ2's goal is to look for recommendations and good practices towards IR in OT. The primary objective of the interview itself is to identify what the respondent thinks is particularly challenging with IR in OT environments as well as identify the current state of practice related to the given organizations IR approach. There are also questions regarding what the respondent thinks is potential solutions or good practices for IR in OT environments, that they necessarily don't practice on the behalf of other factors. Some of the interview questions are open-ended, and some are based on the knowledge we have

gained from collecting the background literature. This is to compare the already identified challenges and best practices to see how they manifest differently or if they do manifest differently in the real world.

The interviews were conducted online via Microsoft Teams. This was the most convenient way, since the company's locations no longer was a limiting factor. The Teams application also provides the possibility to record and transcript meetings , which was utilized for further analysis after the interview. Before each interview, we sent out the invitation to the meeting, which contained the consent form and a draft of the questions that could be asked during the interview. Before we started each interview, we informed that the interview will be recorded and transcribed, double-checking that the interviewee was okay with this. During the interview, we generally followed the interview guide and asked follow-up questions where we felt it was necessary. When the interview had concluded, we summarized the respondents rights according to the consent form and asked for general feedback or if there was something they would like to add. Each interview lasted between one and one and a half hours, depending on how much the respondent elaborated on each topic.

3.4 Data Analysis

In both qualitative and quantitative research, a variety of tools can be supportive, and the choice of tool is not all that critical. The choice of an analysis technique depends on the purpose of the research. Recker emphasizes five common techniques for analysis: coding, memoing, critical incident analysis, content analysis, and disclosure analysis. Coding helps with analyzing and reducing qualitative data to meaningful information by organizing raw data into conceptual categories, where each code is effectively a category where a piece of data is placed. This is performed by assigning a piece or chunk of data a "tag" or a "label." This can be done by organizing data around a concept or theme we identify with the data (Recker, 2021).

In the analysis phase of our research, we consider the coding technique to be the most suitable approach. We intend to use some of the same techniques as we did when categorizing the extracted data for our literature review. We specified coding subtopics in advance in the following three categories: challenges, the current state, and best practices. From there, subcategories of challenges, such as "legacy systems," emerged from the data. This approach allows us to create an organized overview of the findings from the interviews, make the analysis process itself simple, and make it easier for us to compare the data from the interviews with the data we have collected earlier in the background literature while still being open to new topics that our background literature did not cover.

The research question for this consists of two parts: the first part seeks to understand the general cybersecurity challenges of IR in OT, and the second part seeks to understand what measures companies can implement to ensure a successful approach to IR in OT. The first part of the research question "What are the main challenges of IR (IR) within Operational Technology (OT) environments?" will hopefully be answered by comparing the results from the interviews with each other and by comparing the challenges identified in our background research to the challenges identified in the interviews. If a specific challenge identified in our previous research is frequently mentioned by interview respondents, it indicates how widespread the challenge is. If a challenge is noted in both our interviews and previous research, it is likely a well-recognized and common problem in IR within OT. Conversely, if interviewees mention challenges not found in existing literature, these could represent new

findings.

To be able to come up with recommendations on how a successful IR approach should look, it is essential to map what the current state of practises and readiness in this area. The second part of our research question, "What practices can organizations engaged in essential operations implement for a successful approach towards IR in OT environments? ?" will hopefully be answered by looking at the current state of readiness among the participating organizations. By examining how organizations prepare for potential incidents, and comparing their actions and inactions with the literature on different IR approaches, we aim to establish a solid foundation for effective recommendations and practices for successful incident response. We hope to contribute to existing theory by examining practices not mentioned in the literature, and vice versa.

To validate our findings, we will cross-check them by comparing the findings from the interviews with each other and with the background literature to strengthen the validity of the statements. Not only will the validity of the interview findings be strengthened, but the background literature will also get some validity if some of the statements are mentioned in a real-world scenario in the interviews.

3.5 Challenges & Limitations

The main challenge of our data collection is the limited number of people that is suitable for interviewing. We contacted more than 30 potential organizations and only ended up with seven informants for our study. Many stated that they simply didn't have the necessary expertise or a plan they could contribute with in a potential interview. We also called companies that did not answer emails. Often in this scenario did they give out other emails that we could contact them through, but none resulted in a respondent. Two of our respondents explicitly stated that a lot of organizations generally don't know enough about the complex domain of OT tied up to cybersecurity and don't want to address or admit they lack the necessary plans. They also emphasized that incident response in OT poses more questions than answers, suggesting that companies with IR plans may prefer to keep their strategies close to their chest. While it's regrettable that we didn't receive responses from a large number of respondents, because their insights could have benefited our study. Nonetheless, this absence further reinforces the motivation behind our thesis.

While we recognize numerous advantages to employing a qualitative method for this project, there are potential drawbacks. The limitation of qualitative research methods is the subjective nature of data interpretation. Since qualitative data often involves subjective experiences and perspectives, different researchers may interpret the same data in slightly different ways. One disadvantage of qualitative research is the difficulty of generalizing findings to a larger population. Qualitative methods can also face issues considering reliability, this is because the study processes are often contextualized to one case that necessarily cannot readily or faithfully be repeated in other cases (Recker, 2021). It should also be stressed that the interviews with professionals that work with cybersecurity in OT were not carried out to obtain results that are generally representative of all companies that utilize OT. The collected views were collected from industry evangelists; hence, they help us identify the current state, the main challenges, and best practices due to their work in relevant fields of cybersecurity in OT, respectively. In addition, it is necessary to understand that the defined subjectivity can be accompanied by bias and reduce the generalizability of findings. This conciliation is crucial while developing conclusions based on the achieved results.

One of the most significant limitations that applies to us, is the lack of adequate support for evidence. In addition, we have a limited time window, a limited amount of resources to help us get key informants, and, in general, a lack of experience in conducting literature reviews and interviews, these are all factors that will influence our findings. However, we did find seven highly relevant interview objects for this research question that might help us come closer to an answer and might diminish the limitations.

Given our sample size of seven respondents, inherent limitations in generalizability, and the revealingly subjective nature of people's experiences, we choose to take an interpretivist approach. The goal in this instance is not to make broad generalizations but to develop a more nuanced understanding of the interpretation of perceptions by individuals in OT-related IR. Qualitative insights gathered from the interviews should generate rich, context-dependent information that will enable us to understand the subtleties of individual perspectives. Therefore, we shall strive to gather information vital to understanding the essence of how our interviewees navigate the theme's many complexities in unique and diverse ways (Rehman & Alharthi, 2016).

3.6 Ethical Considerations

Data collection involving humans does not present the same potential harm to participants in information systems as it does in biological or medical studies. However, ethical clearances must be applied for and approved prior to starting any research activities that involve humans (Recker, 2021). Before we started our interviews and data collection, we sent a formal request to the 'Kunnskapssektorens tjenesteleverandør' (SIKT), which was approved within a few days. This was done so we could use what the informants say in our report, but also to protect and inform the interview subjects.

In our qualitative approach, we have based our research on the ethical principles of the National Research Ethics Committees (NREC), which specify the principles (1) respect, (2) good consequences, (3) fairness, and (4) integrity in ethical research (Committees, 2019).

NREC has further developed several general guidelines for ethical research. They specify that the general guidelines of ethics cannot replace subject-specific guidelines but should serve as a gateway to the principles and concerns of research ethics. In our research, we have, since day one, been on the quest for the truth. We have tried to the best of our ability to be truthful to the subjects we interview and have given them insight into our interpretation of what they have said. Our research will have a high academic quality. As researchers, we do assess a certain degree of competence, and we will, to the best of our ability, try to make the end result have a high quality standard, which will be shown in this report. Our interview subjects have voluntarily consented to be a part of this project and were sent the consent form before we carried out the interviews. The empiric data we assessed from the objects is treated with full confidentiality and is being handled according to the form approved by SIKT. We are aware that we have full responsibility, considering the integrity and trustworthiness of this report. We are also aware that fabrication, falsification, plagiarism, and similar serious violations of good academic practice are incommensurate with such trustworthiness. The report has followed APA7 standardization considering good reference practice, which we have adhered to to the best of our ability. This is to show other researchers respect and credibility for their work. Finally, we will follow the laws and regulations that apply to the field of study (Committees, 2019).

Chapter 4

Findings

In this chapter, we present our empirical findings based on information generated from the seven interviews. The chapter is divided into two sections, organizational practices, which covers what the respondents mention is part of their IR efforts and plans as well as what they think are important practices. The second part is Challenges; this part covers what the respondents mention as the most prominent challenges they face on the topic of OT IR. This approach to presenting our findings is based on our research questions: RQ1: What are the main challenges of Incident Response (IR) within Operational Technology (OT) environments and RQ2: What practices can organizations engaged in essential operations implement for a successful approach towards IR in OT environments? The chapters are further divided into subtopics, make them more readable and understandable considering the concept of the thesis. The information presented here will be further analyzed and discussed in Chapter 5, Discussion, in an attempt to answer our research question.

4.1 Organizational Practises

4.1.1 Laying the Groundwork: Incident Preparedness

Organizations that have established policies and procedures for how to handle potential cyberattacks against OT can be said to have started the journey towards maturity in the field of cybersecurity in OT environments. It is to be said that the degree to which these policies and procedures are maintained and refined differs from one organization to another, and also defines how well they are prepared for a potential attack. The respondents in this study show a difference in the amount of preparation they have done towards their IR preparation within the OT realm. The root of this can have many reasons.

Respondent 4 says they have contingency plans to cover their IR within OT. They use a framework called proactive staff methodology, where one looks at worst-case scenarios early in the process. It often requires substantial time and effort to ensure that plans are in place that address the unique aspects associated with the OT environment. Often guided by Nasjonal sikkerhetsmyndighet (NSM) guidelines or other recognized standards like MITRE or OWASP, enabling them to have some solid principles and plans in the case of a scenario.

Considering the possibility of a playbook for incidents in OT, respondent 7 highlights challenges because of the uniqueness of OT. He says that they have a playbook for IT incidents,

but not for OT incidents. This is partly because OT events are quite unique, with different backup systems and systems in different locations. He suggests that parts of the ransomware playbook for IT can be used to some extent for OT incidents, but they do not have a specific one for OT. Furthermore he discusses the risk of spreading outside the local network is very small in OT-environments. This means that the response strategies and playbooks must be adapted to this difference, e.g. by assessing whether it is necessary to intervene immediately or whether one can wait and observe the situation more closely.

A consistent observation throughout the interviews is the importance of asset management, as emphasized by respondent 1:

"The most important thing is to identify yourself; you need to understand what you have so you can protect it."

This underscores the necessity of a fundamental understanding of both the assets you possess and their value in order to prioritize the appropriate level of security for them. According to some of the small and medium-sized businesses we interviewed, cybersecurity is often not prioritized when it comes to resource allocation in companies. So one needs to understand how to prioritize, to protect valuable resources and systems.

Annual penetration tests and risk assessments enable these organizations to identify possible threats and vulnerabilities within the OT systems. Respondent 2 stated that if they buy security mechanisms from supplier A, they buy penetration testing from supplier B. Primarily, this organization's proactiveness could ensure that its systems are hard to compromise, as they have the ability to prepare and defend themselves against threats. Additionally, the organization is subject to continuous improvement, with guidelines and procedures changing constantly in a bid to match the threat landscape and technological changes. The organizations conduct regular exercises, often at various escalating organizational levels. Not only do they run technical exercises, but these organizations also involve middle management and top leadership to have a holistic view of preparedness. They also invite third-party vendors to some of these exercises to maintain objectivity about their level of preparedness. Therefore, they can rapidly assemble their resources anytime an incident occurs, thus ensuring minimal liability on their squeals of operation. Respondent 5 highlights the benefits of including tabletop exercises in training to prepare for specific incidents. He describes the exercises like this:

"Think of it like a board game, where some are very experienced and they give you a specific scenario. They ask you what you do in a given scenario, and they can give you further tasks to think about as you go, like, the attackers have now infected this system as well; what do you do?".

Respondent 5 further adds that upon the exercise conclusion, the players are presented with results on what went well and where they can improve.

Respondent 7 also highlighted the importance of training and testing their responses to cyber incidents. He mentions that there are typically two training events a year where the focus is general preparedness, while normal cyber incidents can occur once or twice a year. These events can be internal, external, or a combination of both. When it comes to training, he describes how exercises often are organized by external professionals. As with respondent 5, they perform exercises in the form of tabletop exercises where they are given different scenarios. The aim of these exercises is to understand the roles of those

involved, identify available resources, and strengthen the interaction between different actors. After the exercise, the participants undergo an evaluation to learn from the incident, and a summary is drawn up and distributed to all involved. The respondent emphasizes that the training of potential scenarios is the most important part of IR, noting that this is how one can test if everything goes as it should. He mentioned that he really wants more of this training within the field because of the lack of attacks that are against OT compared to IT, which might make them vulnerable if an actual attack occurs. They have also created courses that are developed to separate IT from OT, explaining why one has to be extra careful with certain components and systems in OT environments. The course is on a lower level and explains the difference between IT and OT and why it is important to be attentive to the differences. He further says that this is a mandatory course and that they also have other training activities related to cybersecurity, such as microlearning. Their approach helps the organization identify strengths and weaknesses in the response process and ensures continuous improvement in preparedness against cyber incidents.

Respondent 3 mentioned the need to consider scenarios such as dependency on a single fiber line through a vulnerable area. This shows the specific kinds of risk assessments needed in OT that might not be as critical in IT. Several of the companies interviewed mentioned having established clear procedures for responding to specific cyber incidents, such as ransomware or denial-of-service attacks. Respondent 2 states that they have clear procedures developed for the cyber attacks they see as the biggest threat and those that they are most likely to be exposed to at some point in time.

Some other organizations are relatively early in their development of contingency plans toward a solid IR plan. In this case, the organization may have been focused on other aspects of the run-of-the mill, such as growth and product development. Therefore, they have little to no time to invest in the management of cybersecurity. However, they have made the decision to include it as part of other measures, with a security focus added to annual exercises and collaborations with external partners helping them understand cyber risks better. The common challenge among any of these organizations was the lack of clearly defined responsibilities and procedures for how to handle cyber incidents. These also include criteria for the prioritization of events happening in the OT systems and the lack of continuous training and awareness among the employees. The results indicated an increased willingness to address potential cyber attacks against OT.

Risk analysis and constant revision and refinement of security procedures were unanimously agreed upon as essential to being competitive in the new threat state and technology environment. These are not only means to uncover and control today's threat action but also ways to be prepared for tomorrow's weaknesses as technology and threat shapes revise. Due to the potential consequences of incidents not just involving data loss in OT environments, ranging from physical harm to environmental harm, the stakes in cybersecurity are intense. The respondents stress that the risk analysis should be thorough and ongoing. Often categorizing them with numbers and colors based on the probability and possible damage. Respondent 7 also emphasizes that this kind of categorization is their baseline for knowing all their possible threat vectors and their network, with help from IDS. He outlines that their SOC runs 24/7 and handling all the alerts. They categorize them as low, medium, high, or critical and send them back to the team if they are high or critical. He says that it is important that there is a human view on the alert, because there are false alarms that they might be aware of. These alerts might be integrated as part of the OT system as a functionality. It is therefore important that they are not removed before viewed, considering it might damage the system. The respondent tells us that not all viruses are dangerous, and prioritization is important in this kind of field and environment. He told us a story about a minor virus they recognized that had been there for 20 years, which they just decided to let stay as long as the control

systems worked. They concluded that the investigation of removing it would have a bigger threat potential for the system than leaving it there. Since it had been there for 20 years without affecting the systems. On the other hand, if the alert is critical, they call out to their CSIRT, which involves both IT and OT personnel to handle the situation. But if there is a cyber event in the production plant that has the potential to cause a fire, emissions, or other things that can affect health, safety, and the and the environment (HSE), in this case, they are involving people, considering their contingency plan, and activating its procedures. So they have to have parallel crisis teams that are handling different kinds of incidents but also supporting each other based on the situation.

By continuously revising and updating the security procedures and measures, organizations can adapt to changes not just in technology but also in the direct work of cyber adversaries. Regular revisions of the security ensure that security measures evolve at a pace that matches or outruns that of potential attackers, thereby better safeguarding critical infrastructure. Because of the change and dynamic nature of cyber threats, static security is often not sufficient. The respondents emphasize the importance of a lifecycle approach to cyber security. This does not only involve updates of defense measures and mechanisms against new attacks types but also revising recovery and response strategies to ensure they remain effective under the pressure of an actual incident. These regular audits and reviews are essential, as they identify gaps in the existing security framework and provide insight into areas that need enhancement.

4.1.2 Roles and Decisions: Managing the Crisis

The research on responsibility allocation and decision-making for an organization's IR plan within OT shows a wide variation, which depends on the company size, resources, and external partnership. There are companies with comprehensive internal systems where the team has been assigned clear roles and the range of decisions that role can enforce. On the other hand, were there respondents we talked to who lacked internal preparedness and made full or partial use of external services. Without clear plans for their response in case of an incident.

Some companies have implemented extensive procedures considering the role distribution for an incident. They have documents and mandates that people can follow in the case of an incident. These will portray what each department is allowed to do, almost without getting consent from upper management. In larger companies with access to internal or external SOCs, these might be the first ones to respond to the potential attack, and they are then allowed to quickly check the actions they are allowed and not allowed to engage in. Respondent 4 refers back to this proactive stab methodology that they use to map scenarios, giving sectors a management starting point. The interviewee does not imply any direct challenges to their decision process but does note that cooperation is of essence. In most cases, it is the SOC that takes responsibility, but as things escalate, this can also mean that other departments assume control and decide the larger decisions. Another company use a method where the catcher of the attack or error was automatically made responsible, and from there, the person needed to refer to their written procedures to continue. Noting that challenges in both the IT and OT domains have usually been taken care of by the IT team in the earlier days. He further implies that this is not possible anymore considering the large area that OT encompasses when it comes to the scale it covers. Highlighting the challenges, considering involvement in a cross-section of sectors, that need to be addressed.

The collaboration between IT and OT is essential to an effective IR. The respondents dis-

cussed how a lack of coordination and expertise within both IT and OT can lead to vulnerabilities, as when a respondent expresses concern about the robustness of systems with changes in personnel. The discussions from the interviews highlight that a siloed approach where IT and OT operate independently is increasingly untenable in the face of cyber threats. They reveal that vulnerabilities often arise from a disconnect between these two domains. For instance, IT personnel may not always be aware of the unique operational and safety requirements of OT systems, which can lead to misalignments in security protocols and responses. Conversely, OT personnel might not be fully equipped to understand and implement IT security best practices, which are crucial for defending against network-based attacks. Respondent 2 highlighted a specific scenario where the lack of coordination became apparent: during changes in personnel. Such transitional periods may jeopardize systems as the newly incorporated IT personnel might not be adequately briefed about the existing security measures or when there is a lapse in the activities of the OT security personnel. The respondent feared that the security measures would be breached during this period of change, and from this response, it is clear that without effective communication and joint strategies, the functions of IT and OT could compromise the set security measures. This section of the chapter further stresses the critical need for response teams that integrate IT and OT professionals. The teams will ensure the security measures not only comply with the IT else-set requirements but also become applicable and effective in the OT context. Cultivating room for joint implementation and understanding is fundamental to strengthening the security measures for organizations' operations in the environment.

Respondent 7 talks about the responsibility and handling of cyber incidents in OT environments. He describes incidents, such as virus attacks on computers, as being treated as cases that need to be handled. He explained that there is defined responsibility for the detection and handling of such events, and the responsibility can lie with different persons or teams. He also mentioned that he can call several subcontractors if one cannot solve the problems themselves. If the event is classified as more serious, could a team of people with different roles be involved to handle it. He further points out the difference between responsibility and authority when it comes to handling such events. Noting that in emergency situations, it's clearly defined who's got the responsibility and what measurements should be implemented, while in other situations, authority could be more vague, He underscores the importance of clear procedures and defined responsibility for the effective handling of cyber incidents.

Conversely, other companies have difficulty with a lack of internal guidance and insufficient work between IT and OT. Respondent 3 explains their challenges, stating:

"I wouldn't claim that we have a good contingency plan yet, Our network had a cyberattack, but even now, we're still working on setting up a proper IR plan."

Highlighting their ongoing struggle to establish a solid response framework. They rely on external providers to deliver IT assistance, and thus a lack of specific roles produces ambiguity about the incident reaction. The latter businesses frequently have insufficient internal competencies and use the services of external consulting firms to handle complicated or serious acts. Moreover, some organizations enter into agreements with key technology partners to build the Network operations center (NOCs) and SOCs, ensuring regular service availability and the expertise the organization lacks. This issue is significantly prevalent once the firm has taken no action to formalize the IR process. Furthermore, such companies hire their partners to execute decrees and other specialized labor during security incidents.

As for prioritizing incidents to decide who is responsible or allowed to shut down systems, little or no decisions are mentioned in each OT environment. Most of the decisions are based

on a balanced approach; every action must be taken to secure production and operations. Particularly in situations of responsibility ambiguity, decisions can be left for process owners or emergency response teams to act based on the normal conditions framework. Therefore, collaboration with external security services and even national security authorities is common, especially if organizations have no internal competence to make their own decisions. Our findings show a link between understanding possible situations through scenarios, being ready to act effectively, and having a basic understanding of what to do and how to do it. Our findings show that OT environments are likely to have formally integrated systems and a mandate to act, which helps improve preparedness and readiness for collisions.

4.1.3 Early Warning: Detecting Anomalies

The findings indicate that all of our respondents have detection mechanisms implemented in or around their OT environment to detect irregularities. Respondent 1 states that they have implemented most of the regular tools, both passive and active. They also mention that there is a mix of tools that they control themselves and tools that their partner controls. Respondent 2 states that the detection mechanisms that they have implemented are nothing out of the ordinary and describes them as typical network surveillance mechanisms that report to a centralized Security information and event manager (SIEM) solution, as well as other mechanisms like sensors on the OT itself that could also be an indicator of an anomaly. Respondent 7 highlights an important aspect of detection in AV or IDS. On their AV, they have "detect, do not delete," which only reports the detection. So on most of the systems, it only reports the virus, but nothing happens. Stating that they have to do this manually because of their fear of false positives. He further explains that a patch on the AV might be implemented, and it detects a virus that has been there for several years and that it is an important part of the system. The respondent further outlines how their alerts are being documented. How they have set it up is that their logs from the AV are sent to a splunk, which is then sent to the supplier, which is then sent to an event handling system, which generates a ticket. This ticket is sent to their SOC supplier and categorizes the severity of the alert.

Regarding typical or specific signs that the respondents look for in their OT environment to detect cyber incidents, is a recurring answer that they generally look for irregularities and things that are out of the ordinary. Respondent 2 states the following on the topic:

> *"We look for anything that is out-of-the-ordinary. It's simply what you need to look at because it's supported by standard production methodology where you aim to produce as consistently as possible day after day with minimal deviation, and you're looking for deviations. It's the deviation that causes things not to go as expected, and that means we can apply standard understanding of production even into a security context."*

Respondent 4 has similar thoughts on the topic as respondent 2; he states the following:

> *"So what we're constantly looking for are abnormalities, anything that deviates from what is normal. It's not specific to OT. It's general. Are there systems or solutions that have started behaving differently than they usually do? Is there traffic that's flowing in a way it never has before? So being able to detect abnormalities is really the main focus."*

Most of the respondents state that they generally think the employees are aware of their responsibility to warn about irregularities when they show up. Respondents 1 and 3 tells

us that this is part of the training they regularly conduct and that they perceive that the employees are generally good at it. Respondent 2 seemed somewhat hesitant about the subject, as he states: "*Yes and no, in a company with the breadth we have, from unskilled workers in production to highly educated engineers with degrees and beyond. In any case, we have a very wide range of expertise. We have employees from 30 countries, so we have a wide range of cultural backgrounds. We have employees from 60 to 70 years old, so we have people of all ages, so we encounter everything at once. That's one of the challenges. We are a cross-section of Norway in many ways in terms of who works here. And that means that some employees are very good and understand this with early warning and actively do it, while others may still not be aware that this is the case. And that's the way this challenge is: that these are not things you can do once a year; they need to be reinforced along the way.*" Respondent 5 states that he thinks that the employees are generally not good at this; he states that his perception is that many employees have an attitude like "it still works" or "it's not my problem; why should I care?".

Regarding the most common method of identifying irregularities in OT environments, the respondents' perceptions varied slightly. Respondents 1, 4, and 5 stated that they think it is hard to give a definitive answer and that they feel like it is a combination of tools like AV, detection software, and logs, as well as employees who notice that something is off. Respondents 2 and 3, however, seem to be concordant in that they think detection software like AV or other detection mechanisms are the most common way of detecting irregularities.

4.1.4 Resilience in Action: Recovery Strategies

Analyzing the recovery strategies across the different companies makes it is clear that there are common attributes and varied approaches to managing such critical situations. There was companies with fully scaled frameworks and policies for their recovery after a potential attack, as well as unfulfilled strategies that were either in progress or just started.

Many of the respondents emphasize robust backup solutions as an important component of their recovery efforts. Three of the respondents mentioned that they utilize immutable backups, where the backup cannot be altered or encrypted by ransomware or other crypto viruses. Stating the importance of this, on the background of available recovery from a source that cannot be infected or encrypted. As respondent 1 put it,

> "*One of the greatest risks is companies not separating their backups. If you lose control over, e.g., login credentials, and the attacker gains access and encrypts all of your data, there is no way back. Then you either pay them or you wipe everything and start over.*"

Respondent 5 mentioned that they generally try to implement immutable backups where this is possible. He mentions that there are often issues with older operating systems that don't have a snapshot feature, which again makes it difficult to implement these immutable backups.

Companies differ in analyzing attack methods and contagion. Most of the companies divide their IT/OT systems into multiple zones and differentiate with several VLANs. They further use internal or external SOCs or other analyzing experts to analyze traffic and identify sources of infection. Allowing them to contain and manage attacks more effectively. Respondent 7 states that they divide their OT environment into very specific zones that do not have a flat structure. It is very restricted what access the different networks have to each other

and stay in the network that the virus is on. With help from the external SOC, they can try to understand and guess what is safe to keep and what needs to be rebuilt. Respondent 3 indicates a lack of such a plan, acknowledging that they are not "at all" prepared when it comes to analyzing attack methods and that this will have to be outsourced. What we have experienced is that almost all companies do not have the internal resources to analyze and conduct forensics in the aftermath of an attack. In the case of an incident, they call in third-party actors that assist in getting the information that is required or of interest.

Strategies to prevent further damage during recovery also vary. Companies focus on damage-limiting measures such as selectively deactivating parts of the network to isolate them. This is a common strategy that most companies use to mitigate further damage. Respondent 2 compares this to a submarine, where damaged sections are isolated to prevent further spreading of water. Respondent 5 states that they use sandboxing as the chosen method for this; this allows them to test the backups in isolated environments to make sure that the chosen backup is clean. Other companies are less prepared and lack a concrete plan to handle spreading during the recovery phase.

After an attack, it is critical to be able to restore systems to a working state. Some companies have detailed plans describing which system should be restored first and who is responsible for it. This is where the immutable backups come in handy. They also conduct thorough verification to ensure that the systems are clean and functional before they are brought back online. This, of essence, tells respondent 1, 2, and 4, noting that if there is just a smidge of infected data in the system, this can have fatal consequences for the rebuild. Checking all of the components in depth ensures there are safe zones to start rebuilding. Respondent 2 states that if there is an infection in one area, they treat the whole zone as infected. Respondent 4 mentions that this is documented in their "business continuity" plans. Others also mention that if you catch intruders within controlled areas, an idea is to observe and gain information before taking other measures.

4.1.5 Aftermath: Post-Incident Review and Actions

Regarding activities planned to take place in the aftermath of an incident, three of the respondents explicitly mentioned conducting of lessons learned activities. Respondent 4 emphasized the importance of reporting and following-up on improvement discrepancies or measures within their internal framework:

"We always conduct reporting and follow-up on any discrepancies or measures related to why an incident occurred. This is an integral part of our internal framework."

Respondent 2 acknowledges that major incidents is very rare, but highlights the importance of conducting lessons learned:

"We always conduct reporting and follow-up on any discrepancies or measures related to why an incident occurred. This is an integral part of our internal framework. Major incidents are known to be rare, so we have little experience with the need to actually take action, but generally, lessons learned are planned to be carried out. In situations where personnel have been affected, debriefing and support may be necessary, as experiencing such events can be quite burdensome for individuals"

Respondent 1 indicated their intention to notify NSM and the police if they are ever exposed to a cyber attack severe enough. However, Respondent 3 mentions a lack of procedures or plans for post-incident activities.

Respondent 7 says that they always review the events after they have taken place. Further saying that the review of incidents is similar to how they review an exercise, where they try to identify what was handled well and what could have been handled better. He points out, however, that they have had very few incidents in OT environments and thus limited experience with such post-incident activities. Despite the limited experience with real events, he mentioned the importance of learning about all types of events, and he mentioned specific events they have reviewed and written summaries about. The aim is to take the learning further and continuously improve response capacity and preparedness.

Three of the respondents indicate that they utilize a deviation reporting system to document incidents, facilitating post-incident learning. Respondents 2 and 3 highlight that these are general deviation reporting systems that cover everything from fires, people falling and hurting themselves on slippery floors, to cyber attacks. Additionally, three respondents mention their practice of adapting IR plans based on insights gained from previous incidents.

Respondent 4 expresses certainty about having clear procedures for implementing new security measures and ensuring their follow-up. Respondent 2 candidly acknowledges their organization's shortcomings in this regard:

"It's a good question, and I don't think we actually do that well enough, to be honest. The human factor is the main challenge there, very often. So it's not system failures causing things; it's a human factor. Someone has clicked on a link, replied to an email, or lost something. It's rare that there's an attacker coming from outside these days. It's difficult to prove, so conducting regular exercises and maintaining a good security culture, I believe, is the best way to achieve that goal, but measuring it is very, very difficult."

Additionally, Respondent 3 states that they lack any specific procedure to ensure the implementation and follow-up of security measures, relying solely on what their external partner provides as part of their service agreement. When it comes to assessing the effectiveness of the IR procedure and identifying areas for improvement within the process itself, only one respondent acknowledges conducting such evaluations. This respondent is also the one who claims to have clear procedures for implementing new security measures and ensuring their follow-up.

4.2 Challenges

4.2.1 Legacy Equipment

OT's reliance on older technology, which was initially not designed to withstand modern cybersecurity threats, is a concept that requires attention; these systems have proven to be vulnerable for a long time. As more OT systems connect to networks, their vulnerability increases over time. The critical need for uninterrupted service in infrastructure, such as power plants and manufacturing facilities, complicates cybersecurity efforts because it restricts the ability to perform timely updates or maintenance that could disrupt operations,

making these difficult to schedule. Furthermore, OT's operational demands necessitate ongoing, specialized risk assessments between IT and OT teams. Respondent 5 emphasizes the continuous struggle when suppliers no longer support older legacy systems, making it difficult to find the right people with expertise on the systems. Respondent 6 also states that legacy equipment is a significant challenge in OT. He mentions that system owners want to keep older systems running for as long as possible to maximize profits, ultimately resulting in doing the bare minimum when it comes to security. Respondent 6 further suggests that law enforcement should be stricter in this area going forward.

Respondent 1 reflected on past experiences dealing with this in the pharmaceutical industry:

"I have worked with quite a few very old manufacturing systems in the pharmaceutical industry, where there is a lot of legacy and it is very complex to secure systems that initially were not built for withstanding today's threats."

This poses a fundamental challenge in IR, securing systems that were not designed with contemporary security threats in mind. The systems may lack modern mechanisms that are commonly found in newer ones. Responding to incidents against legacy systems can be significantly more challenging without knowledge about them. To counter such weaknesses, he mentioned the importance of mitigation controls as a compensation for the system's vulnerabilities. Respondent 1 also addressed this problem and suggested compensating measures such as firewalls, isolation, segmentation, and surveillance. Respondent 7 endorses these measures, asserting that they have segmented all their networks and can physically isolate the OT networks in the event of a serious IT attack. Their OT-systems could be set to"island mode," as he calls it. IT will then have no possibility of accessing the OT systems. He states that they have two island modes. One mode connects OT-offshore to OT-onshore, allowing them to support the offshore plants from land. They also have a mode that completely isolates the offshore plants, leaving them unable to receive assistance from land in the event of an attack. He says that this mode is their last resort. Noting that these measures are essential and necessary to identify threats or vulnerabilities.

Respondent 2 highlighted a shift in technology that impacts the concept and intricacy of IR, stating:

"Traditionally, IR involved buying hardware with a software component attached." "Today, we buy software that incidentally has some hardware, and the shifted focus requires us to have much more control over security."

This change requires a different approach to IR. Since the system is often integrated so closely with IT and the Internet, it increases its complexity and connectivity. Exposing it to a wider spectrum of cyber threats necessitates a continuous response strategy for management, as opposed to a static approach that could have been sufficient for more isolated, hardware-focused systems. Multiple objects also highlighted the difficulties in updating and maintaining legacy systems, citing the absence of available upgrades and parts as a barrier to maintenance work. The lack of available upgrades and parts is something that further complicates the IR. Teams can struggle to patch vulnerabilities or replace outdated components swiftly after an attack. This lag in response time can be critical where operational continuity and safety are paramount.

Respondent 7 says they have plans and evaluations considering the issue of legacy equipment. They know that many of their systems go out of support or are out of support. Once one

system is out of support, the risk automatically increases. If they, for different reasons cannot change the software that is no longer supported, they have to look at mitigation measurements, as previously mentioned. These could be checking if the AV is still supported in the system, they might reduce or remove the remote access control or disable USB input. Then they document this risk in a risk register, and once a year or every six months they evaluate. Asking themselves under this evaluation, has anything changed considering this risk? Could we do any more mitigation measurements? Can we change it? Could we upgrade? The same respondent are addressing the issue considering changing these kinds of systems. He said that some of the software might only be accessible through one special version of Windows. If they were to change components or systems, it would be an ambiguous project with the amount of testing and potential downtime they would have. This would be their last option, and they will try all different opportunities before it comes to this.

4.2.2 Security Patches and Continuous Uptime

The necessity of continuous uptime was also discussed multiple times during our interviews, especially in light of availability requirements, which pose challenges in the context of IR within OT environments. Respondents agreed that uptime and availability is the most important thing when it comes to production companies. As one succinctly put it:

"Availability trumps all other aspects along the way in a manufacturing company. If we cannot make our product, we do not earn money, and then we are bankrupt. This is why production overshadows everything else."

This is why their maintenance window must be vigorously defended to maintain production efficiency. Respondent 2 emphasizes the strategy to minimize downtime by implementing redundant systems and more robust testing environments, allowing continuous operation even during updates. The prioritization might limit their opportunities for maintenance and updates and can hurt the incident respondents ability to get the systems to adhere to their standards. If the system is not up-to-date, both the chance of an incident occurring increase and the response can be weakened. Respondent 5 states that their customers rely on 100% uptime and that most maintenance on the OT systems on oil rigs is performed during operations in specified time windows. Respondent 5 adds that changes on the larger end of the scale are typically performed when the rig is moving to another location and therefore are not in operation. They further add that if something is highly critical and may affect the control systems, they send personnel out on site.

The balance between the implementation of security updates and the avoidance of operational interruptions could directly or indirectly impact the IR within the organization. To reduce the impact, Respondent 1 suggests an approach that minimizes dependence on external systems and suggests protecting the inside to the best of their ability. That one should build OT in an autonomous way, being the least dependent on enterprise systems, such as outside connections. In this way, one will learn these patch tasks in case of a breach of maintenance agreements. By reducing dependencies, organizations can better control their environments and reduce the attack surface, which can be pivotal during IR and the surface respondents have to deal with.

Respondent 2 highlights the challenge of finding time for updates without affecting production:

"Practically, we have a Christmas stop here once a year." "We take down machines to change bearings, balance rollers, and everything. We make the physical operation optimal for the next period, optimally avoiding unplanned stops."

This seems to be a strategy that many of the respondents utilize, where they search for periods when they can stop, secure, and update their systems. However, the respondent notes challenges within their company regarding this approach. For the shutdown to be feasible, IT systems must be operational to test the IT/OT integrations. Unfortunately, IT also schedules updates during this period, leading to conflicts over update windows. The coordination between IT and OT during these periods has to be robust and requires strategic scheduling. If the planning during these periods does not align, this might impact the response time, increase the risk of failure, or cause strategic vulnerabilities because necessary updates or patches might not be there. Another challenge highlighted by respondent 6 is the ongoing struggle of not being able to introduce security measures due to response time. He emphasizes that security measures such as certain firewall settings simply cannot be brought into some of the systems because they will slow down the signal to the extent that the system will think there is something wrong. Respondent 7 is outlining that while their system is under support, they try to update and patch it every quarter, every six months, but state that it is not possible to do it every month.

4.2.3 Support and Maintenance

Support and maintenance often depend on suppliers and constraints of third-party solutions. In some cases, the suppliers do not understand that they deliver software with inherent bugs and challenges. Considering IR, having software with these issues might slow down the response or create unnecessary situations. As a result, suppliers and possible third-party maintainers are important aspects of the organization to control. Suppliers might not have plans for maintenance or the ability to deliver products with a plan, even though they know how important availability is within OT environments, as outlined by respondent 2. He continues to say the suppliers keep making stand-alone products and emphasizes the need for communication between the suppliers so that there is no contradiction in the product that is received, expressing his discontent regarding this issue. Respondent 2 further outlined the lack of security perspective the suppliers can have with an example they experienced only three weeks ago. He said that their company cannot always handle all the maintenance on the products they buy and is sometimes in need of support from the suppliers. When they are proceeding with the maintenance, they are in need of virtual engineering computers or VPN connections to access the system. To simplify this, the supplier mounted a 4G modem so they could easily access the system anytime they wanted to. The supplier further said that if they needed anything, just give them a call, and they would fix it through this modem. Our respondent seemed frustrated about this situation and explained that this was not how they wanted it from a security perspective. Respondent 7 is saying that they have some of the same issues as Respondent 2, but says that they have tried to meet these challenges by standardizing their suppliers. Stating that they have chosen suppliers many times to get to one that they are satisfied with. Suppliers who fail to meet the company's standards are automatically dismissed. He further states that in larger control systems, they have reliable standard suppliers, but in smaller and less crucial systems, they may be more inclined to experiment with new and innovative solutions, which could potentially lead to unintended consequences.

Other respondents, like nr. 5, specify that they have very strict regulations regarding suppliers. They employ PAM (privileged access management), implementing their own procedures

for granting access to suppliers, and relying on central solutions to prevent any independent access to their systems. When a supplier submits a support case, they establish agreements about the room and equipment they use, and they also monitor and record their actions. They emphasize the significance of support security for their equipment and software, recognizing its potential to complicate the organization's IR. Respondent 7 tells us that they split up the responsibility, considering support and maintenance on their systems. He tells us that their systems have two sides: the application side, where they get support from the supplier. However, when it comes to patching and AV, they either have internal procedures or include other vendors for such OT maintenance. If they need changes on the applicational level of the system, they are totally dependent on the supplier, so if that supplier, e.g., runs out of business, he states that they are vulnerable. Considering the main OS, disks, physical computers, servers, etc., are they handling this themselves.

Respondent 1 explained that if the OT infrastructure is built properly, the chance of having an incident in OT is much lower than in traditional IT. He highlights that OT systems that run autonomously with minimal human interference will make the system well protected. However, he emphasized that the security mechanisms of systems can work against us and that this also makes it more difficult to solve issues and respond to incidents from a distance. Respondent 5 brings up much of the same, as he states:

"Our systems are air gapped and completely isolated from the internet, this is an active choice made by us and our customers. We deem it too risky to send data back and forth from the rig and shore. We also have rigs that are moving around the entire world, often stopping in places where there are no satellites or communications, which makes it physically impossible to send or collect data, requiring support and response on site."

In investments related to security incident management, companies prioritize differently. A risk-based approach is highlighted, where resource allocation depends on an evaluation of the most critical and probable risks.

"It's a continuous prioritization, but we use what is called a risk-based approach"

Illustrating a strategic approach to security investments based on an evaluation of potential threats and their consequences. Another sees this as a challenge because security usually does not have its own budget and is too small to have this. So for their part, they have implicit demands considering their security aspects that have to be maintained. The challenge might be for top management to understand the security concerns and then budget for them.

4.2.4 Culture and Competence

Cultural and competence-based challenges in OT environments were highlighted, particularly in relation to how organizations adapt to the changing threat landscape in cybersecurity. Respondent 4 specifically talks about the challenges in maintaining an adequate level of competence among those who operate and maintain an old OT system:

"The challenge lies in the fact that legacy systems are nearly impossible to patch or fully secure. Additionally, there is the need to consider the expertise and knowledge of those who have operated this legacy equipment for many years, along with the evolving threat landscape."

This reflects a broader issue where older systems are not only technologically outdated, but also require specific knowledge that may be difficult to maintain as fewer new technicians are trained to handle such systems. Furthermore, issues with organizational culture and resistance to change can often complicate the implementation of new security practices and technologies. This was addressed by respondent 3, who said:

"New security practices and technology are just something they don't understand, or it is too uncomfortable to take on."

He further says that it is very costly to change them, illuminating how proposals for upgrades or changes sometimes are met with silence or resistance. It indicates that it is not just technical barriers that hinder improvements in OT security but also cultural and competence-related limitations. Therefore, a strategy that has become more necessary is cultural building and competence development within organizations, so that both new and old employees understand the importance of and are capable of handling modern cyber threats. It is essential that both IT and OT teams have a shared understanding and can work together to strengthen the security of critical systems. Considering ensuring a successful approach to IR in OT environments, it is therefore important to address these challenges, considering the competence gap. It requires a workforce that is up-to-date with modern cybersecurity practices and the systems used within the OT-environment. Culture and competence could substantially reduce the risk of incidents by securing processes for quick detection, response, and recovery.

Respondent 7 highlights that it can be difficult to properly understand the consequences of cyber incidents. He pointed out that it can be challenging to distinguish between whether an incident is actually a cyber incident or something else, and this makes it difficult to understand what is going on and what actions should be taken. Regarding the consequences of an attack, he noted that it can be difficult to know what the worst consequences might be and whether it is right to intervene immediately or to wait out the situation. This requires a good understanding of the context and detailed knowledge of the event, which can be challenging to achieve. He also mentioned a conflict between the interests of IT personnel and those who want to intervene immediately to limit the damage. While IT personnel will usually prefer to gather as much information as possible before making a decision, there may be pressure from others to act quickly to prevent further damage. This conflict illustrated the challenges that can arise when one has to navigate between acting quickly to limit damage and, at the same time, ensuring that decisions are based on a thorough understanding of the situation.

Respondent 5 mentioned that one of their largest challenges is with people, stating:

"We have had challenges with customers from time to time where they have modified the systems we have delivered, which again have opened up for vulnerabilities. The largest security risk posed to our systems are basic USB sticks, which could be infected, where people with good intentions are just going to fix something quickly."

Respondent 5 further adds that one of the main challenges they face is simply ensuring that people follow the processes and procedures that are in place to ensure that the systems stay up and running. He also emphasizes that he believes higher technical competence at management levels would have been beneficial, and emphasizes that a strong security posture from top management is crucial for ensuring a successful approach to IR in OT. Respondent 7 says that they also had an issue with people using unauthorized USB sticks on a vulnerable

system. He highlights one example where an employee had done this exact thing, but luckily the result was good for the company. The employee had used a USB stick in a system that never had AV and had not been patched for 10 years. This employee wanted to get some files out, and when he plugged this USB stick into his normal computer, this computer picked up viruses on the USB stick that came from the OT system. Respondent 6 elaborates further on the topic:

"The lack of overview and foundational hygiene is a significant challenge. Most leaders today are convinced that cybersecurity is taken care of. This often stems from IT, which has this responsibility. There need to be more campaigns and training here, as well as investment in knowledge and solutions that cover these demands."

Respondent 6 further highlights that most people see cybersecurity as someone else's responsibility and emphasizes that this is much like HSE, everyone's problem and responsibility. He further ends with the statement,

"We would probably have solved a lot if our focus had been more on humans than technology."

4.2.5 Attack Vectors

In the academic discussion of security incidents and attack vectors in OT environments, interviews with the representatives reveal a range of concerns for managing potential threats. These interviews shed some degree of light on both experienced and potential security threats. We included this chapter to examine specific attacks that OT environments might face. Many companies lacked concrete examples, possibly because OT attacks are less common than IT attacks. However, other companies could potentially learn from each other by sharing how attacks were managed and identifying major threats.

This was not the primary interest we had in doing these interviews, and most of the respondents did not have too much experience considering attacks or potential attack vectors that they saw as substantial for the company. Although did they have some input on attack vectors that could trigger the IR.

Only one of our respondents stated explicitly that they had personally witnessed a cyber-attack on OT. Respondent 5 mentions that the largest concern they have when it comes to cyber incidents on the OT that they manage is viruses. Respondent 5 states:

"We have had rigs that have had both larger and smaller virus outbreaks; we had an incident earlier where the entire control system and operational systems were infected. We have also had a lot of smaller incidents where our AV has caught viruses. And all this has been in systems that are air gapped and not connected to the internet."

Respondent 6 states that they have never experienced a cyber attack directly affecting the PLCs in control systems. However, he stated that he has witnessed attacks affecting the CCTV systems. This was about an incident that happened on an oil rig in the northern sea. The CCTV system was infected by a worker. This spread quite fast because there are a lot of components connected to this network. The lack of foundational documentation on the networks made forensics and IR incredibly time-consuming and difficult.

From respondent 1, we gained insight into an organization that recognizes the importance of protecting its future OT environment in collaboration with third-party corporations. The representative from this organization expresses an understanding of the risks associated with intellectual property and the importance of data loss prevention. They are preparing for future reliance with experienced security partners. We could tell from the interview that he did not have concrete attacks he was concerned about but more addressed the overall security of the company.

Respondent 7 is highlighting an issue considering securing the communication between the offshore and onshore VPN connections. They found out that their VPN was insecure and had many security holes. To handle this, they contacted their SOC and asked them to continuously and carefully watch out for indicators of compromise (IOC) and the possible port that is vulnerable. While they are patching their VPN and security vulnerabilities as fast as possible together with the supplier, this was mostly considering IT. Their handling of vulnerabilities against their OT is often received as a vulnerability alert from trustworthy sources such as Kraft CERT or other security organizations, saying that firmware components might be vulnerable. When a serious alert like this is received, will they first check if the system that is affected is in use within the organization. If this is the case, a ticket is submitted and a follow-up process is implemented. The first step of the follow-up is to analyze the system topology and consult with system owners to determine the vulnerability. E.g., if the vulnerability demands remote access, is it checked if it is remote access to this firmware? If remote access is unavailable, can they conclude that they don't need to urgently upgrade the system. Updates can then be planned until next maintenance stops, something that saves resources and time. A concrete example that the respondent highlights involves a serious vulnerability in the internet-connected system. Because of the high risk of attacks from external actors, they implemented immediate upgrades with support from the supplier. Illustrating how fast they need to handle if necessary. In cases where the analysis shows vulnerabilities that are not exploitable in their environment, can they choose not to implement immediate measurements. Showing two sides in their approach to vulnerability handling. The respondent also highlights the importance of continuous threat evaluation, especially in light of changes in the global security situation and the threat landscape. E.g., after the Russian invasion of Ukraine, did they perform a comprehensive review of their systems to secure updates and sufficient protection against potential attacks, looking for potential weaknesses and extra mitigation measurements.

In contrast, did respondent 2 have specific concerns about attacks he saw as concerning. He highlights his concern, saying:

"What we are most concerned about is supply chain attacks"

The vulnerability of OT systems is underscored by their dependence on external engineers expertise and software. The interviewee further explains that outdated software is often used, increasing the risk of security breaches. He further added that employees with little to no education or knowledge considering cybersecurity often need to have access to engineers computers with software to control PLCs and also the deepest level of the system. Saying that they are primary electricians and not IT personnel. The problem could be that they run outdated and potentially insecure software on the PLC, and a supply-chain attack may occur. He particularly emphasizes the risk associated with backdoors installed by actors in critical system components, such as SSH packages in Linux systems, which can provide unauthorized access to networks and systems. Respondent 7 is also highlighting his concern considering a prominent attack using USB sticks, where the attack distributes manipulated USB devices to persons they know will use them, e.g., engineers on different plants, which

can lead to a supply chain attack. Where the attack includes transferring malicious software to the systems where the units are plugged in and categorizing this as one of the biggest risks. Further, he points out that "normal" viruses are no longer the biggest threat because most systems have updated AV software. He also highlights examples of complicated attacks, such as Stuxnet, which illustrate how effective such attacks can be.

Chapter 5

Discussions

This chapter presents the discussion of our findings, divided into four parts. The first part covers theoretical implications, comparing our findings with previous research to see if they are supported by existing literature and identifying any new ideas and practices. The second part offers practical recommendations for organizations to ensure a successful approach to IR in OT environments, based on both previous research and our findings. We will highlight the most prominent findings and also address less frequently mentioned but important measures. The third part explores opportunities for future work on this topic, and the final part discusses the limitations of our study.

5.1 Theoretical implications

. Our research dives into the practical aspects of IR in OT environments, as it uncovers a spectrum of strategies, challenges, and organizational affairs. By comparing these empirical findings from the interviews, we can enlighten the multiple critical implications that both inform and challenge existing theory.

The literature emphasizes the importance of creating IR plans tailored to specific incidents (Stouffer et al., 2011). Our findings align with this, as several informants stressed the significance of through and ongoing risk analysis, such as color-coded risk matrix, to identify the potential impact of different incidents on their operations. This supports the theory that a nuanced understanding of risks can enhance organizational preparedness and resilience. Moreover, our findings reveal that many respondents have developed specific plans for various incidents based on their classification. This verify existing theories on the necessity of customized response strategies in OT environments. However, respondent 7's admission that their organization lacks a cyber incident playbook for OT environments highlights a significant gap. This point to the theoretical complexity of OT systems, where high specificity and low generalizability complicate the development of universal response plans.

An intriguing finding, mentioned by respondents, but not explicitly covered in the literature, is the use of tabletop exercises. These exercises can be theoretically significant as they provide a practical method for testing preparedness and identifying weaknesses in a controlled environment. This finding suggests a potential expansion of the theoretical framework on training, incorporating scenario-based exercises as a critical component.

Another notable finding from our informants is the importance of asset management, highlighted by respondent 1: "You need to understand what you have so you can protect it". While this may seem obvious, it is theoretically significant in complex OT implementations. This underscores a need for asset management frameworks within the theoretical context of OT security, suggesting that understanding and managing assets is foundational to effective IR. The literature emphasize the importance of delegating roles and responsibilities for effective incident management. Our findings align with this, as the more prepared companies in our study highlighted the importance of extensive procedures for role distribution during incidents, including clear guidelines on departmental permissions and responsibilities. This support the theoretical framework that structured role delegation enhances incident management effectiveness (Jaatun et al., 2009)

Both the literature and our findings stress the responsibility of alerting relevant personnel when there is suspicion of an incident. One respondent noted that the employee who identifies a potential incident is automatically tasked with notifying the appropriate personnel. This aligns with existing theories that emphasize the need for clear communication channels and predefined alert protocols. The literature also underscores the importance of having relevant personnel ready to receive alerts and initiate IR, whether internally or externally. Our findings reinforce this, noting that companies with access to a SOC, either in-house or outsourced, can quickly receive alerts and initiate response actions. This support the theoretical model that the presence of SOC capabilities enhances organizational responsiveness and IR efficiency (Hirai et al., 2017).

Previous research presents a framework for dynamic responsibility delegation (Hirai et al., 2017). Our findings verify the importance of this framework, particularly in the context of collaboration between IT departments and OT equipment operators. This collaboration is essential for efficient IR, as it bridges the gap between IT and OT expertise. However, our findings also extend beyond the existing literature by highlighting additional motivating factors. One ongoing challenge is cross-sector cooperation, which remains a significant issue. Our findings indicate that a lack of expertise in both IT and OT can create vulnerabilities. The common issue of a siloed approach, where IT and OT operate independently further complicates IR. IT personnel often lack an understanding of OT system requirements, and vice verse, leading to decisions that may not fully address the need of both domains. This siloed approach underscores the need for a theoretical integration of IT and OT knowledge bases to ensure comprehensive incident management. Addressing these gaps requires fostering a collaborative culture and cross-training personnel to understand both IT and OT environments.

Both the literature and the interviews underscore the challenges tied to legacy equipment. Many of these systems have a long life cycle with limited support from the suppliers, something that can make them vulnerable to modern cybersecurity threats (Stouffer et al., 2011). Furthermore, the lack of expertise and specialists that handle these elderly systems present a significant challenge, according to both the literature and the findings. There is increased complexity and a need for new approaches in cybersecurity, especially considering the increasing integration between OT and IT systems. Despite the similarities, are there some substantial differences in the approach that is presented in the interviews compared to the literature. The interviews give more detailed description of specific security measures used to compensate for the system's vulnerabilities. Measurements such as firewalls, isolation, segmentation, and surveillance are highlighted as necessary for protection against threats. They are also essential for identifying threats and preventing incidents from ever happening. This was highlighted by respondent 1, who said measures are important for protecting old legacy systems that are not designed for modern security threats. Additionally, the respondents mention the necessity of a more proactive approach with strategic preparation and risk

assessments to predict and challenge potential threats before they manifest. This includes the implementation of robust testing environments and strategies to minimize downtime by using redundant systems. This exact approach was mentioned by respondent 2, who said that it can allow for a more continuous operation even during updates. The findings imply that an effective approach to cybersecurity in OT systems demands a combination of specific security measures that can be applied to the elderly systems and a proactive strategy that takes their uniqueness into consideration. An integration of a broad understanding and implementation of security measures could help to develop robust and adaptable security strategies in OT environments.

Legacy equipment can create issues considering the IR within OT environments and impact the need for continuous uptime based on how these systems are built up and how they can be managed. Furthermore, both the literature and the interviewees underscore the importance of continuous uptime in these often used systems as a critical factor in production companies and in other critical infrastructure (Carr, 2014). Availability is crucial to avoid substantial economic losses and to secure efficiency in production. It is especially important for industries with thin margins and short production deadlines, where even short downtime can have a substantial effect on downstream operations and customer satisfaction. Moreover, respondent 6 states that certain firewall settings are not possible to utilize due to strict latency concerns. The frequent prioritization that availability has challenges the IR, as highlighted by the respondents. The prioritization of availability can sometimes deprioritize the maintenance and patch management that are urgent for the preparation of an incident.

Drawing upon insight from the interviews, it highlights some differences in their approach to the matter. They point to specific strategies on how to handle updates without impacting production, which we have seen a lack of in the literature. Respondent 1 suggests an autonomous OT architecture that minimizes the attack surface and the dependency of external systems, such as internet connections. This will reduce the attack surface and give better control over the environment during IR. Although the feasibility of this might be difficult, it could be both challenging and resource-intensive. Considering many existing OT systems are already integrated with external systems, transitioning to an autonomous model might require significant investment in new infrastructure and technology. Such an architecture might increase the complexity of the system, making it harder to manage and maintain. Specialized knowledge and skills would be required to operate and troubleshoot. Respondent 2, on the other hand, mentions the use of yearly maintenance stops to execute necessary updates and patches. However, does the respondent emphasize challenges with coordination between IT and OT, especially if IT systems plan updates in the same period. Respondent 5 emphasizes a certain time window where they do the same thing, not yearly but on demand; this was also suggested by Respondent 4. Commonly, the customer or themselves plans to close the window and stop critical operations for a certain period. The maintenance planning and updates must therefore be thoroughly coordinated to ensure that they do not disturb the daily operations. Without this coordination, it can impact the response time and increase the risk of errors or vulnerabilities. The delicate balance between applying security patches and maintaining system certifications and operational integrity is paramount. Because of the risk of performance deterioration and breaches of certifications, etc., this could lead some organizations to avoid updating their OT systems, which could lead to the use of outdated and unsecure systems such as Windows XP.

One side is patching and updating these systems to make them able to withstand the potential threats that are surrounding them. The other side is the support from suppliers and third-party vendors that many of these organizations require to maintain the systems. Both the literature and the interviewees address the challenges suppliers of equipment and systems can confront. Highlighting issues such as inherent bugs and omissions in the software

they purchase. This aspect underscores the importance of organizations maintaining control over their systems. Often, suppliers need to provide on-premises or virtual maintenance, but there may be a disconnect between the security perceptions of suppliers and organizations. If a company lacks stringent policies on handling support and maintenance, this can lead to miscommunications and vulnerabilities and damage the IR. Therefore, how equipment is managed is critical; it not only minimizes potential threats but also ensures the organization maintains control over system operations in the event of an incident. However, does the interviews enrich us with the security measures and practices that they use to handle these challenges, which are not necessarily addressed and discussed in the literature that we have found. The respondent mentions different strategies, such as the use of privileged access management (PAM), which includes strict routines for how suppliers get access to their systems. It includes centralized solutions where they do not have independent access, and all of their activity gets logged and monitored. This measurement has been seen as essential so that the company has control over the system they run. On the other side, it demands a deep understanding of complex systems; they are also costly and resource-dependent, which can be factors that make it difficult for minor companies to implement. It could be easy to just trust the suppliers blindly. In this case, written agreements could be important for legal reasons if something goes wrong.

The challenges of each company, all depend on what kind of organization they run and what measures they have implemented to withstand them. The infrastructure of the company is therefore very important to address so one can know what risks they are up against. We have talked to several respondents, most of whom have different infrastructures. Some organizations isolate much of their OT systems, which makes them more resistant to attacks and decreases their attack surface. Respondent 5 addresses human factors as one of the greatest security challenges there are. They have a more isolated infrastructure, and therefore, negligent or malicious insider threats are seen as one of the greater risks. On the other side, there are companies that might have a more open infrastructure and can be more easily targeted by remote attacks. Both the literature and the interviews highlight the importance of competence and the necessity of a robust security culture for effective handling of OT security. Respondent 4 highlights the challenge of maintaining sufficient competence among the operators of elderly OT systems. He mentioned that those who have worked with these systems for a long time often lack an updated understanding of today's threat landscape, which creates a competence gap. Respondent 3 adds that he sees an increase in resistance against new security practices and technology, especially if they could be perceived as complicated and costly to implement. Understanding and approval from upper management could also be hard to receive for the same reasons.

The detection of irregularities is stated by (Jaatun et al., 2009) to usually be identified in one of two ways: either by coincidence, where someone notices something unusual, or by detection software like IDS or AV software. Among our respondents, there were varying answers to what they mentioned as the most common way of identifying irregularities. Nevertheless, our findings show that both IDS and AV, as well as noticing that something is wrong, are mentioned by the informants as common ways to identify irregularities. We have seen a wide range of how the interviewed organizations perceive their employees. Respondents 1 and 3 indicate that the employees are generally good at notifying about irregularities and the responsibility they have; respondent 2 is hesitating around this question, and respondent 5 is more pessimistic about it. However, most organizations do carry out exercises to measure their preparedness and to maintain the consciousness of their employees. They do tabletop exercises where the participants are presented with specific scenarios and tasks that challenge their ability to handle complex security events. The results from these exercises give insight into what works well and what needs to be improved. One of the companies simulated something on the network and challenged the SOC to find this potential threat. They also

outlined that they have paper exercises and are sending out regular phishing emails that test the entire organization's preparedness level. The findings imply that an effective approach to cybersecurity in OT environments demands an integrated strategy that combines technical competence development, a strong security culture, and planned maintenance and management of systems. The interviews give practical examples of how cultural and competence-based challenges could be addressed through specific measurements and procedures. The comparison between the literature and the findings from the interviews highlighted different aspects, considering their approach to attack vectors against OT. Both the literature and the findings address challenges and risk tied to cyberattacks within the OT-environments (Kanamaru, 2020), but we have seen a shortage of respondents saying that they have experienced severe attacks. Respondent 5 expresses his concern about viruses as their largest threat. He mentioned concrete examples where control systems have been infected, even though the systems are air-gapped and disconnected from the Internet. This illustrates how vulnerable the OT systems can be, even when they are isolated from external networks. An interesting finding mentioned by respondent 7 is that they don't always remove viruses from infected systems, as this may result in doing more harm than just leaving them there in cases where the virus does not affect the normal operation of the system. Further, a large number of the respondents highlight the importance of protection in the OT environment, especially having third-party actors they can call when things really backslide. This was also addressed as an important aspect in the literature review we conducted (Jaatun et al., 2009). None of the respondents have the capacity to handle everything when it comes to IR. It would not be financially sustainable to have this specialized competence available 24/7. There is a fine line between where a company should draw its line on protection, comparing it with what they are protecting and their economic status. This reflects a broader strategy for handling security incidents by cooperating with experienced security partners.

Furthermore, the importance of damage limitation during the recovery phase is mentioned as a critical factor in both the literature (Jaatun et al., 2009; Kanamaru, 2020) and in our empirical findings. The literature mentions that the ultimate goal is to prevent harm from expanding. Respondent 2 emphasizes the importance of this by comparing it to a submarine, where the damaged sections are isolated to prevent the further spread of water. Respondent 5 highlights something that is not explicitly stated in the literature. He stated that they use sandboxing within the OT environment for this purpose, which allows them to test backups in isolated environments to make sure that they are clean before restoring the main systems. Another similarity between the literature (Security, 2009) and the findings emphasize the importance of having good backup solutions. However, our empirical findings expand on what the literature says by mentioning a specific type of backup solution that can be beneficial. Immutable backups are mentioned by several of our respondents as a robust backup solution that cannot be altered or encrypted. However, respondent 5 emphasizes that there are limitations to immutable backups on legacy systems. The importance of learning from and improving from previous incidents is emphasized in the literature (Stouffer et al., 2011). The literature further highlights the importance of adapting to emerging threats and the insights learned from previous incidents. Our findings correlate with this, as several of our respondents emphasize the importance of conducting lessons learned in the aftermath of an incident. The literature also emphasizes the importance of generating reports for each incident, which can be useful for potential incidents that may occur in the future. This is also highlighted throughout our findings; several of our respondents mention that they utilize a deviation reporting system that includes the reporting of cyber incidents.

5.2 Practical Implications

The best decisions during an incident are made when the organization has already prepared guidelines for the incidents that have the highest likelihood of affecting the organization at some point in time (Jaatun et al., 2009). Even though the findings indicate that there is generally consensus on the importance of having a response plan in place among the respondents, does it also indicate that not everyone has an IR plan for OT in place. This may be self-explanatory for some, but having a set plan with clear guidelines is crucial to ensuring business continuity and successful response and recovery efforts if an incident were to occur.

The literature suggests different measurements and methodologies for effective IR handling and the importance of preparing in advance to both respond quickly and prevail in incidents. NIST's guidance for handling security incidents highlights some tools and resources that could have practical implications for some companies. This includes communication and facility tools such as contact information for other IR teams and law enforcement, as well as smart phones for support outside of office hours and onsite communication. Further are incident analysis machines and software, such as removable media with reliable versions of software for evidence gathering in the systems, as well as digital forensics stations for creating disc pictures, saving log files, and storing other relevant incident data and important resources. Incident analysis resources could include port lists, documentation for OS and applications, as well as an applicable base line for expected network, system, and application activity. Incident suppression software, such as access to pictures of clean OS and application installers for recovery purposes, is also crucial. Many IR teams also create "jump kits," which could be a portable suitcase with the necessary equipment for an examination. This equipment could include many of the just-mentioned resources, and NIST suggests avoiding borrowing their sets for security reasons (Stouffer et al., 2011).

Security culture is a frequently discussed topic within cybersecurity, and as our findings indicate, this applies to OT security as well. Respondent 5 states that people are one of their greatest challenges; he mentions that customers often modify systems and often use USB sticks in the systems without hesitation, which further strengthens this argument. Both respondents 5 and 6 bring up the importance of a top-down approach to security and emphasize that the leaders and upper management must go forward as good examples for the others to follow. Respondent 6 highlights the need for more campaigns and training within the OT realm and states that a lot of the problems they face would probably have been mitigated if the focus on humans had been larger than the focus on technology. We often hear about IT security courses within companies, which include phishing tests, etc. Respondent 7 explicitly states that they conduct internal campaigns on good security hygiene within OT environments. These courses could potentially make people think twice before inserting USB sticks into computers that run control systems, and many companies could most likely benefit from introducing such awareness campaigns.

Delegation of roles and responsibilities is emphasized by both (Jaatun et al., 2009) and our findings as a paramount factor in the preparation stage of IR. The most prepared companies that participated in the study mention that they have well-established procedures covering role distribution during incidents. As mentioned earlier, our findings mention that cooperation across departments is of essence. However, there are challenges related to cross-functional teams mentioned by our respondents. To streamline the process of role and responsibility delegation for those struggling with this, a dynamic framework is presented by a Japanese university (Hirai et al., 2017). The framework defines clear roles and responsibilities for staff of different departments involved in IR efforts. The framework highlights

different tasks and authorities in each step of the IR process. Incorporating this dynamic framework into response efforts makes for a more streamlined and straightforward approach to role and responsibility delegation and may help eliminate much of the confusion and siloed approach of the IT department and the operational staff mentioned in our findings. It is important to note, however, that implementation of this framework may not be suitable in all organizations and may also require organizational changes and training programs to ensure that all staff members are familiar with their roles and responsibilities. The guide on ICS IR by homeland security (Security, 2009) introduced in our literature review may be a beneficial guide for organizations that struggle with role and responsibility delegation. The guide includes several staff members and describes their roles and responsibilities in the context of IR.

During our literature review we identified a framework (Smith et al., 2021) that proposes the use of a capability map as an effective method to assess the organization's readiness and identify gaps in performance. None of our respondents have mentioned that this is something they use or explicitly mention as an area in which they struggle; however, we still think that it can be a beneficial tool for many organizations to identify what areas need improvement or where third-party expertise is necessary. The use of a capability map can aid in pinpointing exact areas that require additional resources, training, expertise, or additional security measures to be implemented. This straightforward approach can help streamline organizations' prioritization processes and resource allocation and improve the overall readiness of their IR capabilities. In addition, the capability map can be a helpful tool for tracking progress over time. By regularly assessing the organization's capabilities through the use of a capability map, they can monitor changes in their state of readiness and help them make sure they are up-to-date and ready to face the ever-evolving landscape of cyber threats. The literature (Chockalingam, 2021; Ying et al., 2015) also mentions several frameworks designed to streamline the decision-making process during an incident. Nevertheless, none of our respondents mention that they make use of any framework to make the decision-making process more effective. One of the frameworks presented in our background literature is "Using Decision Trees to Select Effective Response Strategies in Industrial Control Systems." (Chockalingam, 2021). The framework can aid organizations in evaluating their response strategies with a systematic and clear method for determining their options for response by assessing different incidents likelihood and potential impact based on a foundational, unwanted incident that has occurred. By utilizing this, the organization can make informed decisions based on clear guidelines in a timely manner.

The literature shows that detection of alerts in OT environments is important to document throughout the whole response process. It states that documentation is important to estimate the severity of the incident, understand the scope, and identify the affected ones. The documentation should include details of what happened, which systems were involved, what damage occurred, and how the incident developed. Noting that the documentation also should include false alarms to analyze and improve the response process. The documentation could serve several purposes, including securing all interests with information about the incident, enabling the sharing of best practices, and providing learning based on earlier experiences, giving a base for post-incident analysis (Jaatun et al., 2009). An effective method for incident and accident analysis is, according to the literature, the STEP method. This method uses graphical representation to identify sequences of events. Then place the events, their impact, and how they were handled in a diagram, including this sequence. The relationship between the events and what caused them should also be identified and included in the diagram, connected with arrows. Using this STEP diagram, organizations could identify root causes and weak points that contributed to the incident. These weak points should be further analyzed and countermeasures suggested on a technical, human, or organizational level. Afterwards, the evaluation of the IR process should proceed, which is an important

part of the learning phase. This evaluation should include an assessment of the effectiveness of the IR plans, involving relevant actors, the adequacy of procedures, and communication effectiveness throughout the whole process. Questions that could be asked could include: Did the IR plan go as planned? Were all relevant actors involved at the right time? Is there a procedure or tool that could have helped? Was the communication effective throughout the process? Through this analysis, organizations can identify potential areas for improvement in their security processes and implement necessary measures to strengthen their preparedness against future incidents. Documenting for this degree is resource-demanding and not eligible for many organizations. Many of the respondents have said that their capability to do in-depth forensics to analyze the incident is limited. Many have noted that they call for help from other actors to gather the necessary information to use the incident for learning reasons. There are, of course, many factors that play a part in these kinds of situations, but a practical implication for organizations could be to do this to a certain degree that suits their capabilities (Jaatun et al., 2009).

Our findings indicate that the importance of implementing detection mechanisms in OT environments is common knowledge. The literature emphasizes how IDS and log analysis often detect malware. However, detection becomes more difficult after the onset, whereas cyberattacks are often camouflaged. The literature highlights an important strategy to aid in this; even though the findings indicate that utilizing detection mechanisms is common (Maglaras et al., 2018), no one mentions the importance of a defense-in-depth strategy. This strategy includes layering multiple security controls to minimize risk by slowing the attacker down. This gives the monitoring services more time to detect and respond to potential threats. By implementing this approach, organizations can make sure that no single point of failure exists, as there are multiple mechanisms in place. Another factor identified in our findings that helps prevent the spread of malware from system to system is network segmentation. Respondent 7 highlights the importance of avoiding a "flat network structure" and mentions that they are splitting the network up into different zones that are not interconnected, making it easier to contain the virus. As discovered in our empirical findings, organizations approaches to setting up their OT environments differ greatly. Some have their OT systems completely air-gapped; others are dependent on an internet connection in one way or another. Respondent 7 states that they utilize something they call "island modes," which enable them to disconnect the OT systems from their IT systems on demand. This is implemented as a security measure to prevent further spread during incidents, and it is essential to have this possibility if an organization's OT environment is reliant on an internet connection. An interesting finding related to malware, as mentioned earlier by respondent 7, is the fact that certain viruses or malware may not interfere with or affect any of the operations. He states that certain viruses have been in some of their control systems for 20 years without interfering with the operations. It may therefore be beneficial to investigate the consequences the malware inflicts on the operations before eradication in certain scenarios. This may be more suitable when a virus has been running on a system for many years; however, this is because the system is then known to have run for many years without issues. Respondent 7 further highlights the importance of "detect, do not delete" on AV solutions because of the threat of false positives. This is due to the fact that the AV solution may delete essential files that can impact operations. This is an important factor to consider when introducing AV solutions into OT environments, and manual evaluation is the way to go to mitigate this threat. Respondent 7 also mentions that they have the ability to remotely disable USB inputs on the machines that run the OT systems. Considering that this is a way of infiltration that many fear and one of the ways that makes OT systems vulnerable even though they are disconnected from the internet, it is a measure that can aid in mitigating the threat of malicious USB sticks when it is difficult to control every action of all employees.

As uncovered in our empirical findings, the importance of knowing what you have through asset management is an essential part of the preparation phase of IR. To be able to protect yourself, you must know what you are in possession of. If a security incident were to occur and the given organization has proper asset management measures in place, such as specific plans for their different assets and how they may affect each other, the responders have a better chance of getting the affected assets up and running again much more effectively. In addition, proper asset management should make it easier to identify affected assets during a breach, as well as assess the extent of the incident in a more effective way. Respondent 6 stated that he has experienced challenges with this firsthand during an attack on an oil rig. He mentioned that the lack of documentation on the network made forensics and response incredibly time-consuming and difficult. Had proper asset management been conducted here, could it most likely would have simplified the forensics and recovery efforts. Another important aspect of protecting your assets is to diversify the use of third-party vendors. As respondent 2 stated, they buy security mechanisms from supplier A and penetration testing from supplier B. This helps with maintaining a degree of unbiasedness during the penetration tests, which is beneficial. Another benefit of diversifying third-party components and managing risk with third-party vendors is the minimization of damage done by supply chain attacks. If one of the suppliers were to have their systems compromised, the risk of all the organization's systems being affected is greatly reduced when all of the third-party systems are not supplied by the same vendor. Another aspect of the supply chain that worries respondent 7 is the spreading of malware via USB sticks. He emphasizes that infected USB sticks are what they are most worried about, and he states that this poses the risk of malware spreading uncontrollably between interconnected systems. The risk of this increases further as different third-party systems are utilized. A beneficial aspect involving third parties identified in our findings is the inclusion of tabletop exercises. Furthermore, training plays an essential role in IR efforts. Respondent 7 highlights that there are very few incidents that affect their OT systems and therefore emphasizes the importance of training. This is to know what to do in the event of a real cyber incident because of their limited real-world experience. By incorporating tabletop exercises into the IR training, we get to put the organization's IR efforts to the test with the involvement of a skilled, independent third party. These exercises involve simulations of real cyber incidents, in which the participant does not get to prepare themselves beforehand. This can help organizations identify blind spots and areas that need improvement in a safe environment. These exercises can serve as a valuable addition to IR training and be a helpful way to identify gaps in current IR efforts.

During recovery after an incident, it is essential that the backups utilized are clean to prevent further damage during the recovery efforts. As discussed earlier, our findings highlight sandboxing as a good way of preventing this. In this way, organizations can make sure that the backups are clean and not infected by testing them in an isolated environment. This way, organizations can enhance their confidence in knowing that their backup is reliable and not contaminated. Another important aspect related to recovery is the integrity of the backups themselves. As identified in our findings, the immutable backup is prominently mentioned by our respondents as an important measure. By utilizing immutable backups as part of the recovery efforts, one can make sure that the backups have not been altered or encrypted by malware and can act as a failsafe mechanism for data restoration. It is important to note, however, that there are limitations to immutable backups regarding legacy systems, according to our findings.

5.3 Future Work

Based on the findings of this master thesis, there are multiple fields that could be in need of future research to strengthen the IR in OT environments. The future work should focus on developing and testing concrete tools and frameworks that can support organizations in handling unique challenges tied to OT environments. An important field for future research could be the development of a holistic framework for IR that is tailored for OT environments. This framework could inherit some the practices we have identified in this study. Testing and validating the framework through pilot projects in different OT environments would be essential for securing its efficiency and applicability.

Further research should also address the challenges that not entirely were mapped in this thesis. This includes an examination of specific technical and organizational barriers that could make the IR efforts difficult. It could potentially be useful to study how different types of OT systems and their unique characteristics are impacting security handling, as well as identify innovative solutions for these challenges. This thesis has limitations considering the amount of respondents we could get hands on and therefore limits how representative it is for other organizations. Therefore, another important path for future work is to include a broader spectrum of organizations in the research. By including a broader scale of industries and types of OT environments, the research could give a more representative picture of the challenges and the best practices. This will also contribute to the development of more generalizable and robust solutions that can fit different organizational contexts.

Future research could additionally focus on improving the cooperation between IT and OT departments. This has been an issue we have seen through most of our interviews. The different departments have separate languages with different perspectives and preferences. This includes the development of integrated approaches to secure seamless communication and coordination between these departments, especially during IR. An examination of how cultural and organizational factors are impacting the collaboration could give valuable insight to strengthen the preparedness of the organization as a whole.

5.4 Limitations

While our study has provided insights into the realm of IR in OT environments, all studies come with their own set of limitations. One of our most prominent limitations where the amount of respondents we could get our hands on. Although this was not because of the lack of effort. We did conducted seven interviews with various organizations involved in essential operations, each lasting from an hour to an hour and a half, and tried our best to get hands on more. However, this study could have generalized more if it were including participants from a broader range of industries and improved our insights. This would have given the study a more holistic view of companies engaged in essential operations OT IR capabilities.

The interviewees were more of less all asked the same questions based on the interview guide, with the exceptions due to the nature of semi-structured interviews. However, how deep each respondent went and their level of transparency when responding to our questions varied greatly. Some respondents gave thorough insights and acted as if they had nothing to hide, whereas others were more conservative and did not elaborate as much on the different topics. Therefore is it important to note that there could be information the respondents possessed which they did not want to share. Also limiting the information that is accessible

through this thesis. Another limitation is the fact that one respondents business is not yet in operation. This means that some of the statements are based on how things are planned out to be and not necessarily how they are done.

It is also important to note that we have not identified every article that could be of relevance to this study. This is due to factors such as time constraints, available resources and the accessibility to certain sources of information. Even though we state gaps in the literature compared to our findings, can this be because of disregarded articles that could be essential. Therefore is it impossible to say with confidence that all relevant literature or interview subjects are included. The thesis will and can only be based on the literature and interviewees that we have mapped. Our findings present recommendations on IR practices for OT. However, it is important that these are just our findings, and complete OT IR efforts cannot be based solely on these recommendations. There are certainly more aspects that need to be considered for a successful IR capability.

Chapter 6

Conclusion

This master thesis has explored the most vital challenges for IR in OT environments as well as the solutions essential organizations practice to counter some of these challenges. Through a qualitative approach, we gathered substantial data to enlighten the complex aspects of IR in OT environments. The data was structured around five phases: preparation, responsibility and decision, detection, recovery, and post-incident activities. Here are our concluding findings to wrap up this thesis.

Preparing for incidents is a critical phase for having an effective IR. The data shows that it is crucial to have a clear and comprehensive plan so organizations are prepared when incidents occur. Identifying potential threats and their impact on operations is step one. Through risk assessments, organizations could map their most vulnerable points and understand which events could have the largest impact. This part is essential for understanding the resources you should protect and how they can be impacted in the event of an incident. Having an overview of critical components and systems, as well as their state and security level, is crucial for assessing their security needs. The complexity of OT environments, where many of the systems are elderly and not designed for modern security practices, is thought to be an issue. However, this assessment gives a basis for prioritizing security measures and resources, something that is essential for allocating their focus where it is needed the most. A challenge that is working against these organizations is the steady-shifted threat landscape. It is therefore important that the assessments are updated and tailored to the potential threats. Therefore, testing these measurements and the overall preparation is key to checking if the security mechanisms are in place and if people know their part in case of an incident. The tests should simulate realistic scenarios and help organizations evaluate their response plans, identify weaknesses, and improve cooperation between teams.

One thing noticed in the preparation phase is the importance of people knowing what to do during an incident. What roles they have and who they contact if there is a necessity for additional help. Procedures for responsibility and decision-making is therefor crucial. This includes a dynamic and adaptable framework that is fit for numerous kinds of incidents. The challenge is to ensure that all involved parties understand their roles and responsibilities, especially in complex OT environments where IT and OT might have to tightly cooperate. Effective cooperation between these departments is necessary to avoid vulnerabilities that could occur from a siloed approach. The key is to have satisfactory communication and cooperation across departments with third-party vendors and upper management, which will contribute to an effective response.

Detection of irregularities is a critical component for organizations to notice an attack, and

also important to stop incidents from ever happening. Both IDS and AV software have been mentioned as common tools to detect possible threats. An important aspect of these kinds of software is to have a “detect, do not delete” approach for avoiding false positives impacting the operation in a negative way. The challenge is to ensure that all the security layers are working together and that there are no single entry points that are vulnerable. Implementation of multiple security layers to minimize the risk and give more time for detection and response against potential threats can stall adversaries accessing their system. Other measurements should be segregation of the networks so the organization can more easily have control over potential compromised parts, which will also help the organization recover more swiftly.

The recovery requires secure and reliable backup solutions. Immutable backup systems are highlighted by most respondents as robust solutions for ensuring that the data cannot be changed or encrypted by malicious software. Testing backups in isolated environments, known as sandboxing, is an effective method for ensuring that they are clean before they are restored to the main systems. It is important that the resources required for creating and maintaining such isolated environments are accessible to the organization. Having dedicated, secure testing environments where the backups can run without the risk of impacting the production systems. These backups have to be unchangeable and protected against unauthorized access or modification, something that secures their use as a reliable source for the organization’s recovery and as a failsafe mechanism. The important factor is to make sure that the backups are available and compatible with the legacy systems, which might lack support for different mechanisms. This demands surveillance and maintenance to ensure that the backups are always in a state where they’re recoverable.

Generally is wisdom from previous incidents vital for the continuous improvement of security procedures. Multiple respondents mentioned the importance of implementing “lessons learned" activities and using a deviation report system for documentation of incidents. This gives room for adapting and improving IR plans based on actual experiences. Documentation of each incident is important for generating reports that can be used in future incidents, securing the response to gradually get better. Systematically reviewing the course of events, identifying what went wrong and what worked well, and implementing improvements based on this analysis is a continuous process. Most of our respondents have said that doing technical forensics on OT systems is a difficult job that most of them require outsourced help to perform. The measure that is important is focusing on having resources for thorough documentation and analysis, as well as continuously updating their response plans based on new insights.

IR in OT environments is more challenging than in IT environments. This is because of their unique demands for continuous operations and the elderly legacy systems that are used. OT systems are often critical for the operation of industrial processes, and one fault could have grand economic, human and security-related consequences. All the challenges make it all the more important to have clear and comprehensive plans for incident management. Our findings show that organizations that implement thoughtful practices in preparation, responsibility and decision, detection, recovery, and post-incident activities are utterly rusted to handle the complex challenges that come with incident management in OT environments. Through regular exercises, clear responsibilities, and robust security procedures, organizations can improve their preparedness and response capability and thereby better protect their critical operations against potential threats. This underscores the importance of a holistic approach to security that implies consideration for the specific needs and challenges within OT environments.

Appendix A

Consent Form

Vil du delta i forskningsprosjektet
«Hendelseshåndtering av industrielle kontrollsystemer»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å kartlegge hendelseshåndteringen av industrielle kontrollsystemer i relevante bedrifter. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette prosjektet har som formål å utforske cyber-relaterte utfordringene som er knyttet til hendelses håndtering av industrielle kontrollsystemer. Vi skal hovedsakelig se på hvilke løsninger som er best egnet mot disse utfordringene. Intervjuene våre vil omhandle hvilke løsninger og utfordringer bedrifter praktiserer når det kommer til hendelses håndteringen, samt hva litteraturen tilsier er utfordrende og best løsning. Forskningen vår vil gå ut på å sammenligne informasjon vi mottar fra intervju-objektene mot hverandre og litteraturen. Dette vil danne et grunnlag for hva vi kan presentere som best-praksis mot utfordringene vi har kartlagt tidligere

Hvem er ansvarlig for forskningsprosjektet?

Hauk Høegh Krohn (student), Christoffer Strand Arnesen(student) er ansvarlig for prosjektet. Devendra Bahadur Thapa (veileder). Prosjektet gjennomføres gjennom Universitetet i Agder

Hvorfor får du spørsmål om å delta?

Du har blitt valgt som potensiell deltaker i dette prosjektet basert på din stilling, bakgrunn og kunnskap innenfor feltet industrielle kontrollsystemer og cybersikkerhet.

Hva innebærer det for deg å delta?

Dersom du velger å delta i prosjektet, innebærer det at vi samler inn data fra dine svar på intervjuet. Du vil få tilgang på det du har sagt, og mulighet til å rette opp i eventuelle ting du vil endre på.Dersom du velger å delta i prosjektet, innebærer det at vi gjennomfører et intervju der du svarer til din beste evne på spørsmålene vi kommer med. Det vil ikke bli publisert eller lagret noen personopplysninger eller særlige kategorier av personopplysninger.

Dataen som vil bli brukt i oppgaven vil bli anonymisert og det vil ikke være mulig å knytte dataen mot den gitte personen eller bedriften. Vi (Hauk og Christoffer) vil gjennomføre intervjuet, og vi vil ta lydopptak av samtalen. Anslått varighet vil være ca. 60 minutter.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykkettilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Det er kun Hauk Høegh Krohn (student), Christoffer Strand Arnesen(student) og Devendra Bahadur Thapa (veileder) som vil ha tilgang til personopplysningene dine.
- Navnet og kontaktopplysningene dine vil vi erstatte med et fiktivt navn og/eller en kode og lagret ved forskningsserveren ved Universitetet i Agder.
- Vi lagrer all data på en sikker datamaskin, og lydfiler vil bli overført til denne og slettet fra opptaksenhet i etterkant av gjennomført intervju.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes når oppgaven er godkjent [15. Juni 2024] Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres, og lydopptak vil bli slettet fra forskerserveren. Detaljer fra innsamlede oppgaver eller intervjuer kan bli inkludert i masteroppgaven i form av vedlegg og/eller transkripsjoner i anonymisert form.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Agder har SIKT – Kunnskapssektorens tjenesteleverandør, vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Hauk Høegh Krohn ved Universitetet i Agder Mail: haukh@uia.no
- Christoffer Strand Arnesen ved Universitetet i Agder Mail: christofsa@uia.no
- Devendra Bahadur Thapa Mail: devinder.thapa@uia.no
- Vårt personvernombud: Trond Hauso Mail: Personvernombud@uia.no

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via: Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Appendix B

Interview Guide

Generelle spørsmål som må kartlegges før intervju

- Hvordan type styring/kontrollsystem har dere for deres maskiner? SCADA/ICS/PLC
  - Er maskinene tilkoblet nett? Alt? Deler?
- I hvilken grad har dere noen plan for incident response i det hele tatt?
- Har dere et eget cyber response team/IT-avdeling/SOC?

Challenges with OT as a system

- Ved en mulig hendelse, hvordan håndterer deres organisasjon utfordringer knyttet til eldre, utdatert utstyr i OT-miljøer, spesielt med tanke på begrensede ressurser og manglende støtte for moderne sikkerhetspraksiser?
- Ved en mulig hendelse, hvordan håndterer selskapet deres behovet for kontinuerlig oppetid i OT-systemene, spesielt med tanke på de strenge kravene til tilgjengelighet og pålitelighet?
- Hvordan balanserer deres organisasjon behovet for å implementere sikkerhetsoppdateringer og patcher på OT-maskinvare der det er utfordrende med driftsavbrudd eller ustabilitet?
- Hvordan håndterer deres selskap utfordringene knyttet til support og vedlikehold av OT-systemer, spesielt med tanke på avhengighet av enkelte leverandører og begrensninger knyttet til tredjepartsløsninger?

Prominent attack vectors

- Kan du dele noen eksempler på sikkerhetshendelser eller trusler rettet mot kontrollsystemet, din organisasjon har opplevd i OT-miljøer og hvordan disse ble håndtert?
- Hvordan prioriterer dere investeringer i sikkerhetshendelseshåndtering for å beskytte mot ulike angrep?
- Hva mener du er de største utfordringene din organisasjon står overfor når det gjelder å beskytte OT-miljøet mot cybertrusler?

  - Hvordan beskytter dere dere mot disse utfordringene?

Preparation and planning

- Har dere etablerte retningslinjer og prosedyrer for håndtering av et mulig cyberangrep rettet mot OT-miljøet i bedriften?
  - Hvis så, kan du beskrive hvilken prosess selskapet følger for å etablere disse retningslinjene og prosedyrene?
- Kan du utdype om retningslinjene selskapet ditt har på plass angående menneskelige ressurser, informasjonsutlevering, kommunikasjon og tildeling av myndighet?
- Hvor ofte gjennomfører organisasjonen din øvelser for å teste og forbedre planene for håndtering av cyber hendelser?
  - Hva er hovedmålet for disse øvelsene?
  - Hvordan sikrer selskapet ditt involvering av alle relevante interesser i disse øvelsene?
- Kan du beskrive en hendelse hvor øvelsen var vellykket, evnt mislykket?
- Hvordan klassifiserer organisasjonen deres potensielle cyber-risikoer rettet mot OT-miljøer.
- Hva er de viktigste komponentene i planleggingsprosessen for håndtering av hendelser?
- Hvordan involverer dere interessenter fra drift, ingeniørvirksomhet, IT, ledelse, juridisk og sikkerhetsavdelinger i planleggingen for håndtering av hendelser?
  - Eksempler?
- Hvordan integrerer selskapet ditt ulike ferdigheter i sine håndteringsteam for hendelser og hvordan fungerer dette i praksis? (IT/OT samarbeid).
- Hvilke metoder brukes i håndtering av hendelser rettet mot OT-miljøer?
- Hvordan vil du vurdere klarheten (readiness) til hendelseshåndtering teamene og hvilke gap vil du si det er?

Decision making

- Har dere noen retningslinjer/modeller/verktøy dere følger eller bruker for å ta effektive/gode beslutninger?
  - Eks. Deskriptiv (Hva har skjedd, hva skjer nå), prediktiv (Hva vil skje), prescriptive (Hvordan respondere, algoritmer osv.)
  - Decision tree
- Hvordan prioriterer dere håndtering av hendelser i OT systemene og hvilke kriterier/vurderinger legger dere til grunn for denne prioriteringen?
- Hvilke utfordringer opplever dere vanligvis i forbindelse med beslutningsprosessen under hendelser i OT-miljøet, og hvordan håndterer dere disse utfordringene?

Responsibilities

- Hvordan er ansvarsfordelingen definert når det gjelder hendelseshåndtering innenfor OT i deres organisasjon?
- f.eks. CSIRT, Nettverks admin, System admin, OT ansvarlige som Prosess/kontrollsystem ingeniører osv.
- Hvordan sørger dere for at ansvarsfordelingen er tydelig kommunisert og forstått blant de som håndterer OT-hendelser.
- Hvordan håndterer dere situasjoner der det oppstår uklarhet eller tvil om hvem som har ansvaret for en bestemt hendelse i OT-miljøene?
- Er det noen konkrete utfordringer du har opplevd rundt ansvar og rollefordeling i incident response for OT miljøer?

Detection

- Hva slags deteksjonsmetoder for hendelser i OT miljøet er implementert i deres organisasjon?
- Har dere konkrete planer definert for hvordan dere skal reagere på ulike hendelser? som for eksempel ransomware og DoS.
- Hva opplever dere er den vanligste metoden for å fange opp hendelser? IDS, AV, tilfeldig av en ansatt?
- Opplever du at de ansatte er klar over deres ansvar om å varsle om uregelmessigheter når de oppdages?
- Hvilke typiske tegn ser dere etter i deres OT-miljø?
- Hvordan håndterer dere situasjoner der deres interne team mangler nødvendig ekspertise, eller hvis hendelse er mer alvorlig enn først antatt?

Recovery

- Kan du ta oss gjennom hovedkomponentene i selskapets gjenopprettingsplan etter et cyberangrep rettet mot OT-miljøet/komponenter?
- Hvordan analyserer organisasjonen deres angrepsmetoder og smittsomhet for å formulere gjenopprettingsplaner?
- Hvilke strategier bruker selskapet deres for å forhindre ytterligere skade utvidelse under gjenopprettingsfasen?
- Hvilke utfordringer støter dere på når det gjelder å opprettholde samarbeid mellom ulike interessenter under gjenoppretting etter en hendelse?
- Hvilken spesialisert kunnskap og ekspertise kreves for å gjennomføre forensiske undersøkelser av OT-hendelser i organisasjonen deres?
- Kan du beskrive utfordringene organisasjonen deres står overfor når det gjelder å samle inn data og gjennomføre forensiske analyser i OT-miljøer?
- I hvilken grad følger organisasjonen deres anbefalinger fra diverse rammeverk for gjenoppretting og restaurering av OT-komponenter?

- Hvilke prosedyrer har selskapet deres på plass for å sikre at systemer blir gjenopprettet til sin tilstand før hendelsen?

Post-incident activity

- Hvilke aktiviteter gjennomfører dere etter at en hendelse har skjedd?
- Hvordan evaluerer dere den generelle effektiviteten av hendelseshåndterings prosessen for å identifisere områder for forbedring?
- Hvordan dokumenterer deres organisasjon hendelser og ulykker for å kunne lære av dem i ettertid?
- Tilpasser dere hendelseshåndterings-planer og prosedyrer basert på erfaringer fra tidligere hendelser?
- Hvordan sikrer dere at anbefalte sikkerhets forbedringer faktisk blir implementert og fulgt opp?

Spørsmål til slutt

- Hva anser dere som deres største utfordring når det kommer til incident response i OT miljøer?
- Hva tenker du er det viktigste tiltaket eller best practices for suksessfull incident response i OT miljøer?

Bibliography

Adrian Pauna, e. a. (2013). *Can we learn from scada security incidents?* https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents (accessed: 17.03.2024).

Canada, G. (2022). *Cyber threat bulletin the cyber threat to operational technology.*

Carr, N. B. (2014). *Development of a tailored methodology and forensic toolkit for industrial control systems incident response* [Doctoral dissertation, Monterey, California: Naval Postgraduate School].

Chockalingam, S. (2021). Using decision trees to select effective response strategies in industrial control systems.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., et al. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 21–44.

Committees, N. R. E. (2019). *General guidelines.* https://www.forskningsetikk.no/en/guidelines/general-guidelines/ (accessed: 09.04.2024).

He, Y., Maglaras, L. A., Janicke, H., & Jones, K. (2015). An industrial control systems incident response decision framework. *2015 IEEE Conference on Communications and Network Security (CNS)*, 761–762.

Hirai, H., Aoyama, T., Davaadorj, N., & Koshijima, I. (2017). Framework for cyber incident response training. *Safety and Security Engineering VII, Rome, Italy*, 273–283.

INCIT. (2023). *It/ot convergence: Challenges and opportunities in 2023.* https://incit.org/en/thought-leadership/it-ot-convergence-challenges-and-opportunities/ (accessed: 15.02.2024).

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*, *2*(1), 26–37. https://doi.org/https://doi.org/10.1016/j.ijcip.2009.02.004

Kanamaru, H. (2020). Requirements for it/ot cooperation in safe and secure iacs. *2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 39–44.

Larkin, R. D., Lopez Jr, J., Butts, J. W., & Grimaila, M. R. (2014). Evaluation of security solutions in the scada environment. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(1), 38–53.

Lees, M. J., Crawford, M., & Jansen, C. (2018). Towards industrial cybersecurity resilience of multinational corporations. *IFAC-PapersOnLine*, *51*(30), 756–761.

Maglaras, L. A., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. J. (2018). Cyber security of critical infrastructures [SI: CI Smart Grid Cyber Security]. *ICT Express*, *4*(1), 42–45. https://doi.org/https://doi.org/10.1016/j.icte.2018.02.001

Marali, M., Sudarsan, S. D., & Gogioneni, A. (2019). Cyber security threats in industrial control systems and protection. *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 1–7.

Meagher, H., & Dhirani, L. L. (2023). Cyber-resilience, principles, and practices. In *Cybersecurity vigilance and security engineering of internet of everything* (pp. 57–74). Springer.

Parsons, D. (2023). *Sans ics/ot cybersecurity survey: 2023's challenges and tomorrow's defenses.* https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/ (accessed: 7.02.2024).

Recker, J. (2021). *Scientific research in information systems: A beginner's guide.* Springer Nature.

Rehman, A. A., & Alharthi, K. (2016). An introduction to research paradigms. *International journal of educational investigations*, *3*(8), 51–59.

Samonas, S., & Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Security, H. (2009). Developing an industrial control systems cybersecurity incident response capability. *Homeland Security Affairs*.

Smith, R., Janicke, H., He, Y., Ferra, F., & Albakri, A. (2021). The agile incident response for industrial control systems (air4ics) framework. *Computers & Security*, *109*, 102398.

Stouffer, K., Falco, J., Scarfone, K., et al. (2011). Guide to industrial control systems (ics) security. *NIST special publication*, *800*(82), 2–26.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of planning education and research*, *39*(1), 93–112.

Yassine, M. (2021). It/ot convergence and cybersecurity. *Computer Fraud Security*.

Yau, K., Chow, K.-P., & Yiu, S.-M. (2019a). An incident response model for industrial control system forensics based on historical events. In J. Staggs & S. Shenoi (Eds.), *Critical infrastructure protection xiii* (pp. 311–328). Springer International Publishing.

Yau, K., Chow, K.-P., & Yiu, S.-M. (2019b). An incident response model for industrial control system forensics based on historical events. *Critical Infrastructure Protection XIII: 13th IFIP WG 11.10 International Conference, ICCIP 2019, Arlington, VA, USA, March 11–12, 2019, Revised Selected Papers 13*, 311–328.

Ying, H., Maglaras, L., Janicke, H., & Jones, K. (2015). An industrial control systems incident response decision framework. *IEEE Conference on Communications and Network Security*, *10*.