# Effects of Organizational Cyber Security Culture Across the Energy Sector Supply Chain

Susanne Barkhald Sandberg[1][0009-0007-6989-5139], Aida Akbarzadeh[1][0000-0002-3142-1583], and Vasileios Gkioulos[1][0000-0001-7304-3835]

Norwegian University of Science and Technology, Gjøvik, Norway
susanne.bs@outlook.com, aida.akbarzadeh@ntnu.no, and
vasileios.gkioulos@ntnu.no

**Abstract.** In critical infrastructure, cyber incidents can have significant impact not only on an organization itself but also on the security of society and safety of the public. In recent years, there has been an increasing number of supply chain cyber attacks, with weak links in the chain commonly exploited as points of penetration. For this reason, it is crucial for organizations to start managing cyber security not only within their own organization, but also across the entire supply chain. To shed light on this challenge and bridge existing gaps, this study investigated the effects of cyber security culture within and among organizations across the energy sector supply chain. Our findings indicate that cultivating a robust security culture can significantly enhance supply chain security practices. Therefore, it is of paramount importance to prioritize efforts towards aligning organizations through the promotion of common understanding and shared values. These concerted efforts are not only advantageous but also indispensable as we strive toward a more secure future for the supply chain.

**Keywords:** Cyber security · Cyber security culture · Organizational culture · Supply chain security · Supply chain cyber security · Human factors· Critical infrastructure· Supply chain risk management.

## 1 Introduction

In the energy sector, many organizations have a technical environment that consists of both administrative systems and operational systems. With increasing digitization, the dependencies on these systems, as well as their supply chains, are becoming increasingly crucial. In these environments, there is often a combination of new and old technology, including industrial control systems and legacy systems. Traditionally, many of these systems were physically separated from other systems through *airgapping* [1]. However, with the increasing interconnection between them today, the distinction is becoming less prominent [2, 3]. This results in increased risk for the organizations, especially considering that many legacy systems were not designed with security in mind. Also the increased use of Industrial Internet of Things (IIoT) has raised concerns about vulnerabilities in operational technology (OT) environments [4].

Additionally, the vulnerabilities in the supply chain are increasing with its complexity. In a complex supply chain, organizations lack visibility and control, which in turn exposes them to a wide range of threats [5]. According to ENISA [6], the number of supply chain attacks has increased rapidly in the last years, and this number is expected to continue to increase further in the years to come. This is challenging as it becomes necessary not only to consider cybersecurity within the borders of an organization, but also to take into account the relations and dependencies with other organizations in the chain. Meanwhile, the mentioned complexity and lack of visibility and transparency in the chain can make it difficult to discover and identify such relations and dependencies. In addition, the consequences of a security incident or an attack may extend beyond the affected organization. As a part of critical infrastructures, the energy sector is of significant importance for modern society. Many of the organizations within the sector rely on the same large vendors, creating interdependencies among them [7]. Hence, the ripple effect of large-scale targeted attacks could have serious impact on society. The relation and dependencies between the different sectors and critical infrastructures further makes it possible for incidents to propagate and have detrimental effects even across different industries. Consequently, supply chain cyber security risk is something to consider not only for the individual organizations or the energy sector, but also for national security [5]. The question is then, how can organizations in the energy sector mitigate these risks? Previous research has mainly been focused on the technical aspects of cyber security, while human aspects have been more neglected [8]. Human and organizational aspects of cyber security does however play an important role.‘
Therefore, to fill this gap, this study aims to investigate the effects of cyber security culture on supply chain security practices and the relation between entities in the chain. In more detail, this work attempts to provide insights into:

- How organizational cyber security culture affects the overview and control of dependencies to other organizations in the supply chain from a preparedness perspective (RQ1).
- How organizational cyber security culture affects the level of trust in other organizations in the supply chain (RQ2).

In addressing RQ1, the study explores security practices related to dependencies to other organizations in the chain, such as the procurement process and security revision. It aims to examine how organizational cyber security culture influences the extent to which organizations have a clear understanding of dependencies and maintain control over them. Regarding RQ2, the research delves into the relationship between organizations in the supply chain and the role of organizational cyber security culture in shaping the level of trust. It seeks to uncover the explicit and implicit mechanisms that contribute to trust-building, including policies, agreements, contracts, and revisions. By examining these research questions, the study aims to shed light on the various dimensions of cyber security culture and how they intersect with supply chain relations and practices. The findings will provide valuable insights for organizations in the energy sector to mitigate cyber security risks and strengthen their supply chain security by emphasizing the significance of organizational cyber security culture. In summary, the main contribution of this paper is as follows:

- Bridges the gap between technical aspects of cyber security and human/organizational aspects in the supply chain;
- Investigates the significance of cyber security culture on supply chain security;
- Enhances supply chain security practices;
- Studies trusted relationships among entities in the supply chain and their impact on supply chain security.

The rest of the paper is organized as follows: In Section 2, we review the related work conducted on supply chain cyber security and cyber security culture. Section 3 describes the methodology used in this study. In Section 4, we present and provide a detailed explanation of the findings. We discuss the implications of our findings and their significance in Section 5. Finally, Section 6 summarizes our conclusions and indicates possible directions for future research.

## 2 Related work

### 2.1 Supply chain cyber security

A literature review conducted by Safa et al. [9] investigates the different aspects of cyber security in the supply chain. The findings highlight the multi-dimensional and complex nature of supply chain cyber security. The authors also notably emphasize the significance of organizational and human aspects of security, in particular the importance of risk awareness, risk identification and security policies. Employee compliance with existing policies is also identified as a crucial factor in this work. In more recent reviews of literature, it has been observed that there has been relatively less research conducted on human factors in supply chain cyber security compared to technical factors [8].

Furthermore, Ghadge et al. [8] conducted a systematic literature review in 2019 to explore cyber risk management in the supply chain. The review encompassed 41 articles published between 2000 and 2017. The study emphasizes that the links within a supply chain can serve as vulnerable points of penetration if they are not sufficiently secured, underscoring the importance of identifying these weak links within the organization. Additionally, the findings also highlight the significant role of employees as a major cyber security risk in the supply chain. As stated in the review, "In both the negligent and premeditated mode, the human factor can pose the biggest and most unpredictable threat to a company's cybersecurity" [8]. Moreover, it has been found that the risk increases when employees from different organizations interact [8]. In the year 2022, Melnyk et al. [12] identified small-to-medium sized enterprises (SMEs) as weak links within the scope of their investigation. They conducted an exploratory research study with the aim of developing a research framework for cyber security across the supply chain.

In addition to cyber security risks and challenges within the supply chain, potential mitigations have also been proposed in research. Ghadge et al. [8] classified such mitigations into three distinct categories, based on the phases of an attack: Pre-attack, trans-attack and post-attack. The mitigations related to the pre-attack phase are further divided into those addressing technical factors and those addressing human factors, where the latter being particularly relevant for this study. Among the mitigations mentioned in the study [8], the following examples are noteworthy:

- Awareness training for employees
- Accreditation against standards
- Information sharing
- Standard guidelines for collaboration
- Formalised agreements between organizations
- Supplier audit
- Risk classification and identification
- Zero-trust policy

Roman et al. [10] additionally proposed international cooperation and coordinated actions by government institutions, as well as establishing guidelines to ensure transparency within and between organizations in the supply chain. They point out that this might also include awareness and security training. More specifically, for preparedness, they suggested approaches using cyberrange and digital twins (DTs).

ENISA also provided recommendations in their 2021 report [6]. They presented good practices for both customers and suppliers in the supply chain to manage supply chain cybersecurity risk, as well as the customer-supplier relationships. However, regarding certain threats, they also highlighted that there might be a need for actions to be taken at a higher level than the organizational one, such as at the national or European level.

### 2.2 Cyber security culture

In a recent structured literature review, Uchendu et al. [11] presented the current work and future needs for developing a cyber security culture. Following the PRISMA protocol [12], the study examined 58 papers from the last ten years, focusing on four specific areas: Definitions, Factors, Frameworks, and Metrics. The findings reveal that a significant part of previous research on security culture primarily focuses on information security culture, with only 10 of the 58 articles specifically examining cyber security culture. Figure 1 demonstrates the distinction between cyber security and information security [13].

Uchendu et al. [11] also show that questionnaires and surveys are the most common research instruments along with theoretical research. The study indicates that a significant portion of the research encompasses a diverse range of participants, while a smaller number of studies focus solely on top management. An interesting finding is that, similar to research on supply chain cyber security,

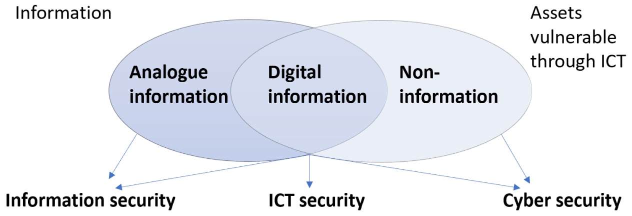

**Fig. 1.** Difference between Information Security, ICT Security and Cyber Security [13]

there has been relatively limited investigation into SME's compared to larger organizations. Besides, there is a lack of research examining the long-term effects of cultural frameworks and approaches in practice.

This literature review also revealed that top management support is the most frequently mentioned factor associated with the development of a cyber security culture, appearing in 34 out of the 58 papers [11]. Other factors are depicted in Figure 2, scaled based on the frequency of their mention in research. It is worth mentioning that while top management support is crucial, it alone is insufficient to build a culture. Other factors, such as trust, awareness, training, and policies, are also vital components in establishing a comprehensive cyber security culture. Notably, regulations are mentioned in only four papers, which is of particular interest in the context of this study.

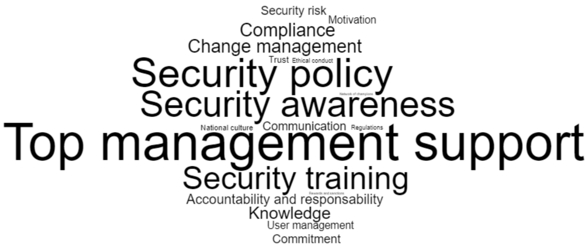

**Fig. 2.** Factors of security culture [11]

Understanding the underlying factors that contribute to the development of a cyber security culture is of paramount importance for this study as it facilitates the examination of potential associations with supply chain security practices. The review of related work revealed a significant overlap between the key factors of security culture and the mitigations of supply chain cyber risk. Notably, there are areas of convergence that encompass elements such as awareness, training, and risk management. This overlap is illustrated in Figure 3. This finding highlights the interconnectedness and shared importance of these factors in addressing challenges within the supply chain context. We will elaborate more on that in the subsequent sections.

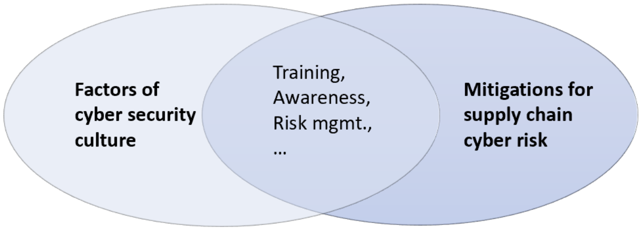
Factors of cyber security culture
Training, Awareness, Risk mgmt., ...
Mitigations for supply chain cyber risk

**Fig. 3.** Overlapping factors

## 3 Method

In this section, we describe the methodology used in the study. The process is divided into three phases including *Problem Identification and Literature Review*, *Data Collection and Analysis*, and *Data Interpretation and Reporting*. Figure 4 provides a visual summary of this section.

### 3.1 Problem Identification and Literature Review

In the first phase of the study, empirical data from the Norwegian energy sector was used as starting point for the research. The objective was to identify challenges, risks and areas in need of improvement in relation to supply chain security. This was studied through publicly available reports from different actors, among others The Norwegian Water Resources and Energy Directorate (NVE), The Office of the Auditor General of Norway (OAG) and The Norwegian National Security Authority (NSM) [14, 7, 5, 15]. Subsequenly, a literature study of related academic research was performed to place the empirical information into a broader context and to shape the theoretical concepts. ENISA's definition of cyber security culture was used as the basis for the theoretical model. In their report, cyber security culture "...refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies" [16]. SME's were also added as a variable to the study at this point, as both reports from the sector and the review of academic research had pointed out challenges around these and their role in the supply chain. In this study we define the term small-to-medium sized as an organization having 500 employees or less.

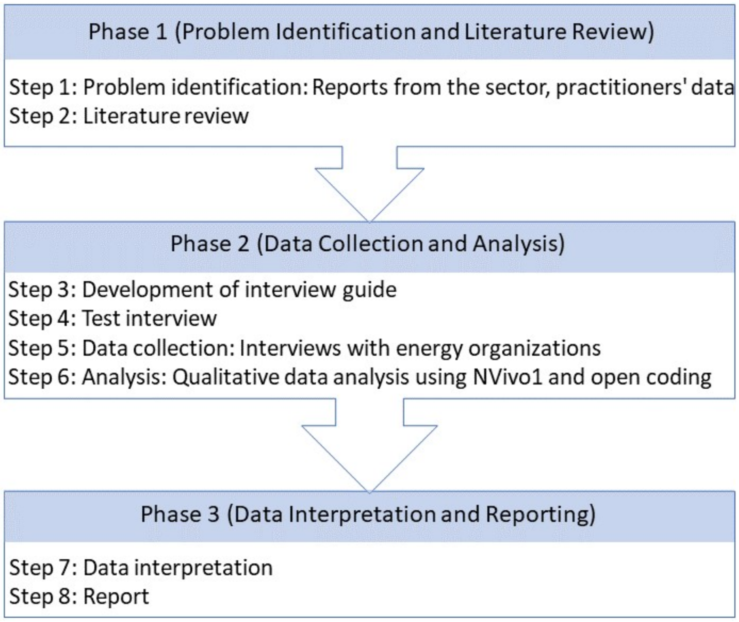
Phase 1 (Problem Identification and Literature Review)
Step 1: Problem identification: Reports from the sector, practitioners' data
Step 2: Literature review
Phase 2 (Data Collection and Analysis)
Step 3: Development of interview guide
Step 4: Test interview
Step 5: Data collection: Interviews with energy organizations
Step 6: Analysis: Qualitative data analysis using NVivo1 and open coding
Phase 3 (Data Interpretation and Reporting)
Step 7: Data interpretation
Step 8: Report

**Fig. 4.** Process

### 3.2 Data Collection and Analysis

Related work has shown that surveys and questionnaires are the most commonly used tools for assessing cyber security culture. Furthermore, reviewing recent studies also revealed several tools for assessing security culture that had already been developed and validated. However, due to the limited research on the combination of cyber security culture and supply chain cyber security in the past, and the need to thoroughly explore the relationship between these concepts, a qualitative approach in the form of interviews was chosen for our study. A selection of the mentioned assessment tools were used as a foundation in the development of an interview guide. In particular, questions and statements from the following references were used to create a database of a total of 245 sample statements: the adjusted Information Security Culture Assessment (ISCA) [17], the Norwegian Digitalisation Agency’s method for assessing security culture [18], CheckIT [19], the ”Workforce”, ”Response”, and ”Third-Parties” dimensions of the Cybersecurity Capability Maturity Model (C2M2) [20]. As a first iteration, all questions that could be relevant to the research questions were identified, categorized and put into a first draft. The number of questions were then reduced in an iterative process. The final interview guide contained a total of 54 questions in four different categories including *Background* (5 questions), *Perceptions of Management and Control* (14 questions), *Incidents and Incident Response* (10 questions), and *Supply Chain Management* (25 questions). Interested readers can refer to [21] for more details on the collected data and questionnaire items,

as they are not included here due to space limitations.
As part of the data collection preparation, a test interview was conducted. This was done for several reasons, with a particular emphasis on verifying the anticipated interview duration and ensuring the clarity and comprehensibility of the questions. The participant in this interview was not part of the study sample. In the next step, interviews with representatives from seven different organizations within the Norwegian energy sectors supply chain were made. The organizations were of different sizes, divided into the categories of SME and LE (Large Enterprise). The study involved participants from these distinct roles:

- CEO
- IT Manager
- Security Architect
- Senior Advisor (Security)
- IT Administrator
- Sales Manager
- Security Manager

The data obtained from the interviews were prepared and analyzed in accordance with Creswell's data analysis spiral [22], a well-referenced approach for analyzing qualitative data (see Figure 5). During the initial review process, in line with Creswell's data analysis spiral, initial thoughts and interpretations were documented in separate comments, distinct from the interview data. In order to further classify the data, the software tool NVivo[1] was used to perform

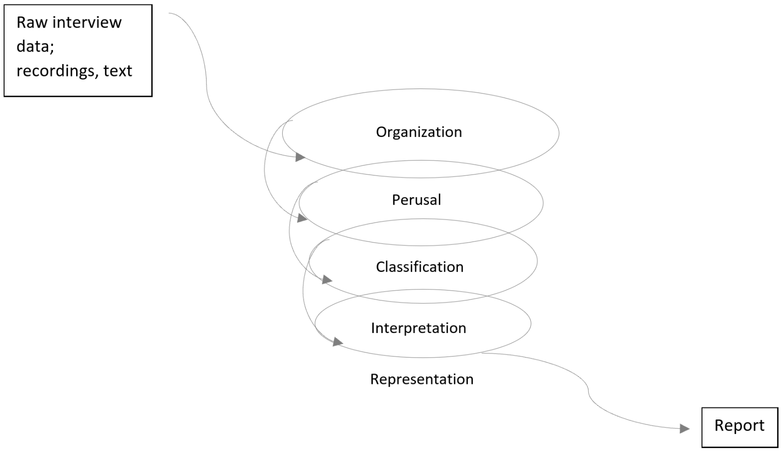

**Fig. 5.** Creswell's Data Analysis Spiral [22]

[1] More information about NVivo can be found at https://www.alfasoft.com/en/products/statistics-and-analysis/nvivo.html

open coding in an iterative process. As a starting point, cases were created for each of the organizations. Responses from each organization was then coded to the respective case. Subsequently, the classifications "SME" and "LE" were created and assigned to cases from small-to-medium sized organizations and large organizations, respectively. Due to their relevance to the RQ's, the codes "Cyber security culture", "Supply chain cyber security practices", "Preparedness", "Trust". "Organization size" were also created. Data relevant to these elements were assigned to the respective codes. Continuing the iterative process, new codes and sub-codes were generated based on the collected data. The goal of this step was to identify any other relevant subjects and potentially uncover any unknown underlying patterns. Figure 6 presents the resulting codes compared by number of references they received.

### 3.3 Data Interpretation and Reporting

In the final step of the classification, identified codes were grouped into themes, marking the readiness of the data for interpretation and reporting. In Section 4 we will delve into a comprehensive exploration of the outcomes derived from these interpretive processes, offering a detailed analysis and insights into the patterns, trends, and key findings encapsulated within the gathered data.

## 4 Results

In this section, we provide a detailed explanation of the outcomes, which will be presented in eight distinct subsections. Each subsection will focus on a specific aspect of the findings, providing a comprehensive analysis of the interview data and their implications.

### 4.1 Governance

The results indicate that cyber security policies and procedures are well established in the energy organizations. With one exception, the results also show that the responsibility for cyber security is perceived to be placed at the top management. Top management support, however, differs much more among the organizations. While most of the larger organizations explain that their top management clearly communicates that cyber security is important for the organization, several from the SME-category express ambiguity regarding their expectations towards employees in terms of cyber security. One explain that top management never challenges them if they are secure enough, but that they rather question if they are spending too much money on security.
Figure 7 illustrates the participants' perception of the most significant motivation for engaging in cyber security work within their respective organizations. The most frequently mentioned aspect was the possible consequences for society in case of a large breach. Legal and regulatory requirements are also important factors, as well as audits, privacy and the EU General Data Protection Regulation (GDPR).

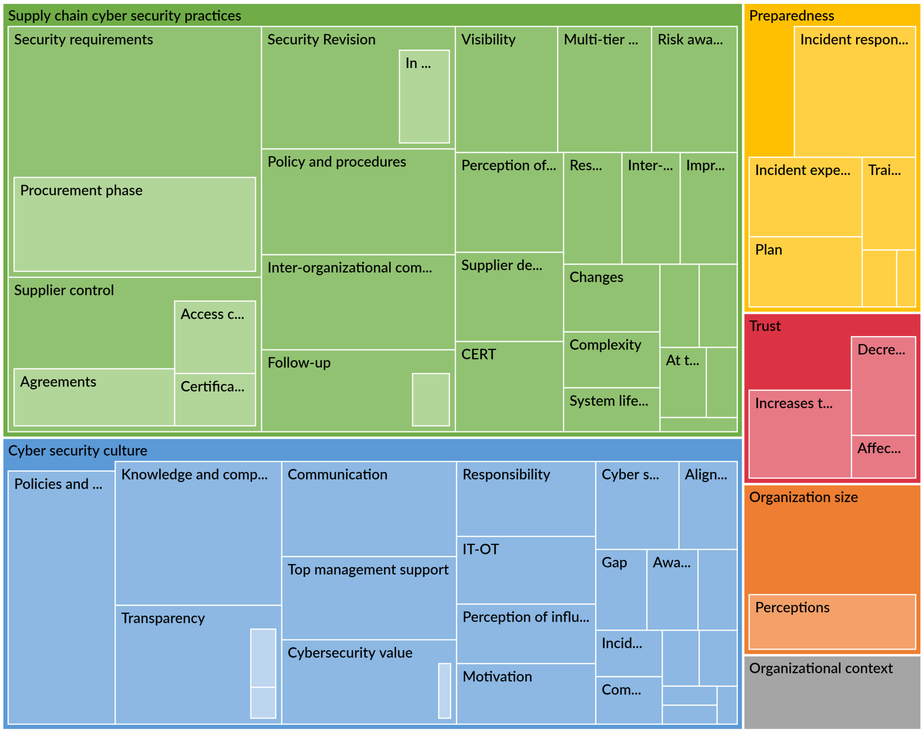

**Fig. 6.** Comparison of Codes by Number of References.

### 4.2 Preparedness and incident response

The results indicate that all participants are familiar with cyber security incidents in the sector, and that these incidents affect their respective organizations to a variating degree. In case of an incident in the sector, at the least, the organizations need to take measures in the form of checking or verifying possible consequences for their own organization. Information sharing among the organizations in the sector is therefore important. A common CERT for the sector stands out as a central point of information sharing, which is highly valued by the organizations. Vendors, however, are not necessarily under the same restrictions and requirements as the energy organizations, and information sharing from vendor to customer organizations might be less structured unless agreed upon.

From a preparedness perspective, vendor control and follow-ups are directly related to the regulatory requirements. The regulatory framework makes strict requirements to power organizations regarding the protection of sensitive power information, and the organizations need to make sure that their vendors fulfill the information security and confidentiality requirements, as well as ensuring the right to control and revise. The results suggest that all organizations have em-

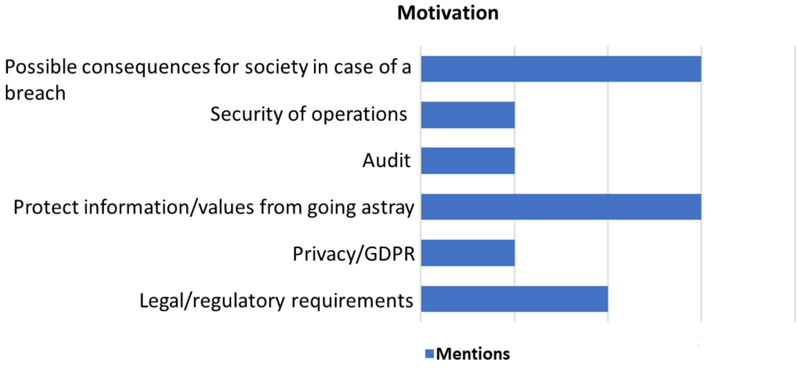

**Fig. 7.** Key motivations for cyber security efforts in organizations

bedded this aspect in their contracts and agreements. They also have important dependencies included in their preparedness plans. In general, policies and procedures that relates to cyber security requirements seem to be well established in the organizations. However, some participants express uncertainty about the extent to which these plans are actually implemented in practice.

### 4.3 Supply chain challenges

Most of the participants state that they only have visibility of the supply chain up to one tier down, two tiers down at the maximum. The depth and complexity of the supply chain, as well as the traceability of components, presents a great challenge for the organizations. More specifically, the following points are mentioned:

- **To know what you are buying.** There are many tiers in the chain and many components in each product. One participant explained this was more challenging in OT than in IT. Another expressed a feeling that vendors barely know what they are selling.
- **Complexity and number of suppliers.** It is challenging and resource-intensive to maintain an overview over time, particularly when dealing with a large number of suppliers, especially those that are primarily focused on delivery.
- **Lack of standardization.** Lack of standardization makes it challenging to know where to make effort.
- **Lack of common understanding.** This was pointed out as a current challenge, particularly when it comes to vendors understanding what it means to deliver to critical infrastructure. A common understanding could push suppliers in the right direction and benefit in the implementation of frameworks.
- **Lifecycle of systems and components.** Keeping all components up-to-date can be a challenge, as some reach end-of-life and are no longer patchable.

- **Gap in competency.** Buyer competency is important in a supply chain. The organization is always responsible for their own data. Misunderstandings of where the responsibility lies is a common challenge from a vendor's point of view.

Further, our results indicate that the organizations have well established policies and procedures to verify that vendors fulfill security requirements when entering agreements, although the specific practices vary from organization to organization. Active follow-ups within the period of contract is however less common, and change management is connected with the following challenges:

- **Updates:** Software/firmware updates from the vendor might be installed without question, vulnerability patches in particular. If these updates are somehow compromised or faulty, it is rarely possible to discover before damage is done.
- **Resources:** Keeping track of the supply chain(s) over time is perceived extremely challenging and resource demanding from the organizations' perspective. It needs to be decided how far down in the chain one should go. Tools and methods for keeping an overview should be considered/developed.
- **Communication:** Communication regarding updates and changes from vendor to customer organizations is challenging and sometimes lacking. Internal communication within organizations is also mentioned as an important point, as the information needs to get to the right people.

### 4.4 Trust

The term *Trust* was frequently mentioned during interviews when speaking of the supply chain. There were also a collection of factors that the participants believed influenced the trust between organizations in the supply chain. The factors are shown in Figure 8.

Transparency and openness, along with dialogue, communication, and relationship, were the most frequently mentioned aspects. These are closely related with honesty. These factors refer not only to the vertical communication of vulnerabilities and incidents within the chain, but also to the exchange of information between the different organizations in the sector. A culture of sharing and openness is necessary across the sector, and the majority of participants feel that this culture is already present today. Some, however, also highlighted that there is room for improvement. The following points were mentioned:

- There is less sharing in OT than IT.
- There have been improvements, but there are still glossy pictures out there when incidents occur.
- Information sharing relies on individuals - Information needs to be lifted to the right people to a larger degree.

A common CERT-function is also highlighted as an important aspect of the information flow. Direct contact between suppliers and their customers appears to be less structured and may benefit from improvement.

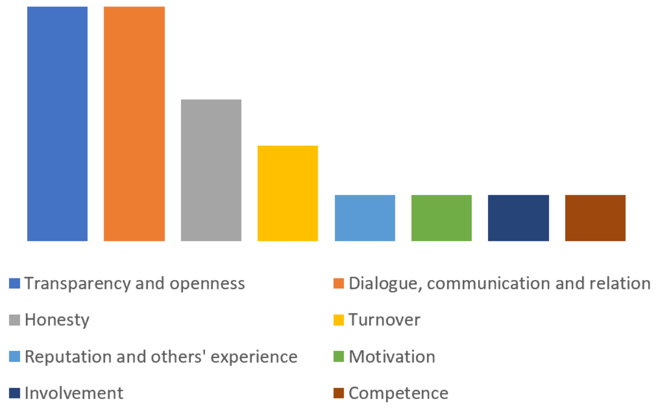

**Fig. 8.** Factors that affect Trust

### 4.5 Looking towards others and propagation of trust

Our results show that especially SME's have a tendency to look to other organizations to a large degree when choosing vendors or making security-related decisions. Vendors with many larger size customers seem to be perceived as more trustworthy. This is built on an assumption that larger organizations have a higher level of security. In organizations where cyber security value was perceived to be at a medium or lower level, the external focus was perceived as a security challenge. This could be due to the fact that decision makers may (1) look to organizations with lower security requirements without fully understanding the difference it makes and (2) look to others to find justification for choosing less expensive systems.

### 4.6 The impact of organization size

SME's were intentially included in the study both because they have been considered weak links in the chain in previous works and that less studies have focused on smaller organizations compared to larger ones [23, 8]. For this reason, the answers were categorized into two groups: SME's and LE's when presenting the results. At first glance, the results seem to support the findings of related work, as they suggest that cyber security is valued higher in larger organizations, and that top management in these organizations have communicated their expectations regarding cyber security to a larger degree compared to SME's. However, there are nuances to consider. Based on the results, participants from both smaller organizations and larger organizations see both benefits and drawbacks of having the organizational size that they have. As already mentioned there are also some assumptions among the organizations that relates to other organizations' size. While the results show that the larger organizations in this study generally take cyber security very seriously, with some of them making efforts to influence their vendors, the findings also reveal that supply chain cyber security poses challenge for them as well. One participant emphasized that they might be large on a national scale, but not on an international scale. They further suggested standing together with other organizations and authorities could be a possible approach to increase their influence on vendors.

Another interesting finding is that while one participant from the SME-category did not believe that they could have any impact on the supply chain because of their size, another from the same category experienced that they could, but by suggesting and presenting good solutions in addition to their requirements. This, however, does require some in-house competency and certain priorities from their side. A third participant from the same category explained that requirements could be stricter in their organization, and that security evaluations were not necessarily followed up by the risk owner even if it showed that the vendor's security was not satisfactory. This is primarily linked to the focus and priorities of decision makers. The diversity of answers suggests that an organization's influence on the chain is determined by a complex combination of factors, rather than solely relying on size and resources.

## 5 Discussion

In this section, we will first discuss the results in relation to the main research questions mentioned in the Introduction. Then, we will also explore additional findings that, although not initially part of the research questions, are still relevant to the topic of cyber security culture across the energy sector supply chain.

### 5.1 Discussion of Main Research Questions

Here, we focus on the discussion of the research questions:

**RQ1:** Our results show that the awareness around the risk of third-party collaboration is high, however many of the organizations are strongly depending on their vendors. The need for what the vendor can offer to the organization outlines the risk or leads to an acceptance of the excess risk. Moreover, organizations in the energy sector find keeping control of their dependencies in the supply chain challenging, both within IT and OT. The visibility is low below the first tier of the chain.

According to the results, organizations have well established policies and procedures for the procurement process. However, the results also indicate that change management and regular follow-ups within contract lifetime is less structured. This is also very resource-demanding for the organizations, considering the number of vendors. Still, it is difficult to discover breaches to the security requirements if they are not actively followed up on. If not, one has to make the assumption that the conditions that are present at the point of entering contract will stay constant throughout the contract lifetime. It needs to be decided how

far down in the chain one should go to keep control and how this should be carried out over time. This depends on knowledge, competency, resources and willingness of both organizations and vendors, and also the perceived cyber security value and priorities within the organization.
From the preparedness perspective, vendor control is directly related to the regulatory requirements that organizations in the energy sector need to comply with. Organizations need to ensure that vendors fulfill the security and confidentiality requirements and they also need to ensure the right to revise. Our results generally indicate that organizations have well established policies and procedures for cyber security and supply chain management, and that they keep control of their vendors through contracts and agreements. However, for some, it is more unsure how well this is followed up in practice. This is a crucial point, as a policy will not be of any value to an organization unless it has an actual effect on practices, especially in a preparedness situation. This suggests that there is still room for improvement, and that building a good cyber security culture could be a way for organizations to cover this gap between policy and practice. However, it would be important for organizations to investigate further the underlying reasons for lack of compliance with policies. There might be several causes, for example risk perception or lack of knowledge, resources or competency. Research has also shown that policy compliance increases when employees are not only aware of the content of the policy, but also why the policies are important [24]. Efforts to identify these factors would ease the improvement process.

**RQ2:** In our study, we have found several factors that are of importance for the trust between different organizations in the supply chain. With the exception of turnover, all the factors are all closely related to the different dimensions of cyber security culture reviewed in related work. As trust itself can be seen as a cultural factor, this is not surprising [25]. Not much related work has looked at cyber security culture beyond the borders of an organization, thus there is a need to separate between the internal trust within the organization and external trust towards other organizations. Transparency, openness and communication stands out among the most frequently mentioned factors that affect the trust between oranizations. It is also found that organizations in many cases could benefit from increased awareness regarding *where* shared information ends up within their own organization. Depending on the nature of the information, it may need to be raised and distributed beyond IT or security personnel. Thus, based on the factors found and their relation to cyber security culture, results suggest that the trust in a third-party would be affected by the third-party's security culture. Nevertheless, the results do not give any clear suggestions to how an organization's own cyber security culture affect the trust in third-parties. The importance of trust in supply chain relations and management is nonetheless remarkable, based on the collected data.
Several participants tended to use phrasings like *"We have to trust our vendors"* or *"We are at the mercy of our vendors"*. The choice of words could indicate that this is more "forced" trust than "earned" trust, in the way that the only

alternative is to trust the vendor. For instance, some pointed to the fact that they have little to no possibility to do security revisions in practice. However, the same participants do feel that they might influence the supply chain through making requirements or in other ways. A possible explanation to this could be that there are alternatives in theory, but not in practice. Many vendors have large, international organizations. It is also worth noting that all participants described to have the regulatory requirements fulfilled through contracts, but that the challenges are more related to how compliance can be verified and followed up in practice.

Our findings also show that trust can propagate within the supply chain. As an example, a participant from the SME-category described that it was common to look to larger organizations in the sector when choosing vendors. Vendors with many large customers are perceived more trustworthy based on an assumption that larger organizations have stricter requirements and a higher level of security. Thus, this assumption leads to implicit trust in vendors. However, the collected data also revealed that the larger organizations find supply chain cyber security challenging. One of the participants from the LE-category also pointed out that simply being large does not necessarily mean that you are great, even if you have some good prerequisites. This is an important point. Every organization is different, and there will be a complexity of factors that have an impact on the general lever of cyber security. Two organizations of the exact same size might have very different values, structure and distribution of resources. It is risky to make assumptions solely based on size, in particular when trust propagates within the chain. Also internally, the focus should be shifted towards other factors. By breaking it down, it is possible to both assess and improve. An assumption that an organization cannot influence their supply chain simply because they are small might lead to less focus on requirements and accepting lower levels of security at the vendor. However the challenge of standing independently should not be underestimated, and it is crucial for all organizations within the sector to be aligned. Efforts to build a strong security culture throughout the sector would in this case be beneficial and would also have vertical effects in the supply chain by a larger influence on the vendors. One of the participants summarized it effectively:

> *" It has to do with raising up those with very low maturity with the help of those with high maturity and make sure it is aligned"*

Finally, a supply chain attack is an attack that takes advantage of the trust between parties. For this reason, organizations need be aware of how, when and why they put their trust in a third-party. Considering the results of our study, it could also be considered to which degree a Zero Trust Architecture (ZTA) approach could be beneficial for supply chain security. The ZTA was developed by National Institute of Standards and Technology (NIST) as a technical approach to cyber security in which there is no implicit trust between parties [26]. However, as stated in an security blog post by Edward Kost, "for the ZTA to have maximum potential, this framework should be implemented both within an organization and throughout its vendor network" [27]. This implies a significant demand and necessitates a cultural shift towards a zero-trust philosophy throughout the supply chain.

### 5.2 Exploration of Additional Findings

**Comparisons to HSE:** During the interview, several of the participants compared their cyber security practices with those related to health, safety and the environment (HSE). The first comparison was related to the value of cyber security, where one participant expressed that they wished that cyber security efforts would be reinforced and supported in the organization in the same way as for HSE. In their organization, HSE was the first point on the agenda at all board meetings. In recent years, the industry organization Energy Norway[2] has focused on HSE, with the aim of making the Norwegian renewable energy industry the best in HSE. In particular, they presented "HMS-Løftet", which is a pledge to lift [3] the level of HSE [28]. The CEOs of the participating organizations must sign and accept five points related to the responsibilities and attitudes they have towards HSE. Energy Norway also made board presentations and guidelines available to the organizations to ease implementation. It is clear that this approach focuses on several of the same factors that are important when developing a cyber security culture, in example top management support, accountability and responsibility[11, 28]. Responsibility is a key word here, as our results have shown that vendors experience confusion from the organizations as to where the responsibility for cyber security lies. Regardless of third-parties, organizations should be aware that they are responsible for the security of their own assets, also those reachable through cyber space. Furthermore, there should be no doubt that top management has the responsibility within each organization. It could be interesting to study the effects of a similar approach as "HMS-Løftet" for improving the cyber security culture across the sector. Of course, this would require efforts from a higher level than the individual or organizational level.

**Alignment:** Alignment is another key word related to the supply chain. Internal alignment is an important factor for internal culture, in terms of the perceptions, assumptions, values and behaviours that exist within the organization. As some of the participants mentioned during interviews, organizations might have different maturity in the different parts of their organization. Some also pointed out that the alignment between IT or cyber security personnel and other employees can be a challenge, which might be caused by a lack of common understanding and a different view on the value of cyber security efforts. Misalignment in organizations can possibly also be caused by conflicting goals, as explained by Parsons et al. [29] in a study of information security decision making. In their study, top management scored less on knowledge, awareness and self-reported

[2] Energy Norway merged with Norwea in January 2023, creating the new organization Renewables Norway (www.fornybarnorge.no/om-oss/in-english/)

[3] Both "Pledge" and "Lift" can be translated to "Løfte" in Norwegian

behaviour. In our case, some of the participants pointed out the two axes of usability and security.

In addition to the importance of internal alignment, our results also clearly show that the alignment between the different organizations in the sector is of great value for the security of the supply chain. A common understanding and shared values should be a goal for the future. This includes not only a vertical alignment (supplier-to-vendor, vendor-to-vendor, and vendor-to-customer), but also a horizontal alignment between peer organizations. Continued development of a culture of openness and transparency should facilitate this process.

## 6 Conclusion and Future work

Organizations in the energy sector hold significant importance as part of critical infrastructure in the modern society. With digitization and increased interconnection, these organizations are experiencing increased risk of cyber incidents. Due to the dependencies between organizations and also between different industries, large scale incidents might have wide-reaching consequences. These consequences extend beyond the individual organizations and can impact society as a whole, as well as pose risks to national security. Therefore, it is crucial to gain more knowledge on how supply chain cyber risks may be managed and mitigated.

In this study, we have investigated the relation between organizational cyber security culture and supply chain cyber security through a qualitative empirical approach. Interviews were performed with representatives from different organizations within the Norwegian energy sector and its supply chain. Our findings indicate cultivating a robust security culture can significantly enhance supply chain security practices. Furthermore, it is of great importance to make efforts towards alignment within the sector though common understanding and shared values.

The study has also revealed several possible areas in need of more research. As participants have pointed out, some organizations experience gaps in maturity and security subcultures within their own organization. It would be interesting for future research to investigate the impact of subcultures on supply chain security to gain a deeper understanding of their effects. Another area of future work would be to identify and investigate a specific cyber supply chain vertically starting from a focal organiziation. Expanding the research to include other EU and non-EU countries and conducting a comparative analysis of the results would provide valuable insights for future research in this field.

## References

1. Krutz Ronald L. Krutz. Securing SCADA systems. Wiley-Blackwell, 2015.
2. Adam Hahn. Cyber-security of SCADA and Other Industrial Control Systems, chapter 4, pages 51–68. Springer International Publishing Switzerland, 2016.

3. Aida Akbarzadeh. *Dependency based risk analysis in Cyber-Physical Systems*. PhD thesis, NTNU, 2023.
4. Colin Topping, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers and Security*, 108, 9 2021.
5. Nasjonal Sikkerhetsmyndighet (NSM). Risiko 2021 - helhetlig sikring mot sammensatte trusler, 2021.
6. European Union Agency for Cybersecurity (ENISA). Enisa threat landscape for supply chain attacks. Technical report, July 2021.
7. Riksrevisjonen. Riksrevisjonens undersøkelse av nves arbeid med ikt-sikkerhet i kraftforsyningen, dokument 3:7 (20202021). Technical Report Dokument 3:7 (20202021), Riksrevisjonen, 2021.
8. Abhijeet Ghadge, Maximilian Weiß, Nigel D. Caldwell, and Richard Wilding. Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, 25(2):223–240, November 2019.
9. Nader Sohrabi Safa, Carsten Maple, and Tim Watson. The information security landscape in the supply chain. *Computer Fraud & Security*, 2017:16–20, 6 2017.
10. Rodrigo Roman, Cristina Alcaraz, Javier Lopez, and Kouichi Sakurai. Current perspectives on securing critical infrastructures' supply chains. *IEEE Security Privacy*, 21(4):29–38, 2023.
11. Betsy Uchendu, Jason R.C. Nurse, Maria Bada, and Steven Furnell. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109:102387, October 2021.
12. PRISMA. Prisma transparent reporting of systematic reviews and meta-analyses.
13. Bjarte Malmedal and Hanne Eggen Røislien. The norwegian cyber security culture, 2016.
14. Elisabeth Kirkebø and Mathias Ljøsne. Ikt-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. Report 90/2018, NVE, 2018.
15. Nasjonal Sikkerhetsmyndighet (NSM). Risiko 2022 - Økt risiko krever økt årvåkenhet, 2022.
16. The European Union Agency for Cybersecurity (ENISA). *Cyber security culture in organisations*. ENISA, Heraklion, 2017.
17. Adéle Da Veiga. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*, 26(5):584–612, November 2018.
18. Digitaliseringsdirektoratet. Veileder for kartlegging av sikkerhetskultur.
19. Stig O. Johnsen, Christian Waale Hansen, Yngve Nordby, and Maria B. Dahl. Measurement and Improvement of Information Security Culture. *Measurement and Control*, 39(2):52–56, March 2006.
20. Office of Cybersecurity, Energy Security, and Emergency Response. Cybersecurity Capability Maturity Model (C2M2).
21. Susanne Barkhald Sandberg. Effects of organizational cyber security culture across the energy sector supply chain [unpublished manuscript]. Master's thesis, Norwegian University of Science and Technology, Gjøvik, Norway, December 2022.
22. John W Creswell and Cheryl N Poth. Qualitative inquiry research design : choosing among five approaches, 2018.
23. Steven A. Melnyk, Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F. Chang, and Derek Friday. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 60(1):162–183, January 2022.

24. Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. A study of information security awareness in australian government organisations. Information Management and Computer Security, 22:334–345, 10 2014.
25. Anna Georgiadou, Spiros Mouzakitis, Kanaris Bounas, and Dimitrios Askounis. A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, pages 1–11, November 2020.
26. Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero trust architecture, 8 2020.
27. Edward Kost. Zero trust as a defence against supply chain attacks.
28. Energi Norge. Kom i gang med hms-løftet. https://www.energinorge.no/publikasjoner/veileder/kom-i-gang-med-hms-loftet/.
29. Kathryn Marie Parsons, Elise Young, Marcus Antanas Butavicius, Agata McCormac, Malcolm Robert Pattinson, and Cate Jerram. The influence of organizational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making, 9:117–129, 6 2015.