Information & Computer Security

Socio-technical challenges in improving cybersecurity in operational technology organizations

Kristian Kannelønning and Sokratis K. Katsikas
Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim, Norway

Received 14 January 2025
Revised 6 June 2025
5 October 2025
Accepted 10 November 2025

Abstract

Purpose – Evidence suggests that the majority of cyberattacks have been made possible because of erroneous or noncompliant human behavior. Nevertheless, many organizations tend to focus their cybersecurity programs on technology, often overlooking the importance of socio-technical cybersecurity controls and practices. The reasons for this and processes to remedy it in organizations making use of IT have been examined in the literature. However, in organizations using integrated IT and operational technology (OT) systems, such as the digitalized manufacturing industry, cybersecurity is often treated with less rigor and attention. This paper aims to identify and analyze socio-technical challenges of cybersecurity in such organizations, with an eye toward improving their cybersecurity posture.

Design/methodology/approach – Two data sources have been used, namely, interviews and a survey, both with participants from the Norwegian Industry. The aim of both instruments was to investigate how cybersecurity is organized and how threats are mitigated, focusing on socio-technical aspects. The interviews investigated how organizations work with cybersecurity and what motivates cybersecurity-compliant behavior. The survey measured the usage and importance of the different security controls found in the NIST Special Publication SP800 - 82r3 "Guide to Operational Technology."

Findings – The results show that organizations should include their OT personnel together with IT in the governance of OT cybersecurity. Communication between IT and OT is found to be a significant challenge. Communication barriers could stem from a lack of cybersecurity knowledge among personnel working with OT. Organizations should, therefore, invest more in specific OT cybersecurity training to bridge the communication gap. With increased efforts in specific training, it is expected that the extent of workarounds should decrease and that deviations found between best practices and the current usage of security controls should improve. By investing more in training, classified as a social element of the socio-technical system (STS), the needle will move toward a balance between the socio- and the technical dimensions of STS, which should yield the highest security outcome.

Research limitations/implications – This study does not give explicit advice nor does it uncover new in-depth knowledge regarding how organizations communicate internally and to what extent IT and OT cooperate; it only reports and discusses the views of the participants. The results of this study should be of interest to practitioners in both IT and OT cybersecurity. Future research should investigate, among others, how cybersecurity is organized and how communication is done within OT organizations.

Originality/value – This study uncovers new information as to how OT industry organizations organize and prioritize their cybersecurity efforts with a focus on socio-technical aspects; it examines if there are deviations between IT and OT systems cybersecurity and investigates how these affect the overall organizational goal of

Funding: This paper was funded by Norges Forskningsråd No. 310105; Norges Forskningsråd No. 323131.

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-01-2025-0018

cybersecurity; and it reveals some of the challenges that such organizations face in achieving improved cybersecurity.

Keywords Cybersecurity, Operational technology, Socio-technical system, IEC62443, Cybersecurity controls, Compliant behavior, Cybersecurity program, Cybersecurity training

Paper type Research paper

1. Introduction

In organizations operating digitalized operational technology (OT) systems, cybersecurity has often been treated with less rigor and attention than those operating purely IT systems. This lack of attention to cybersecurity within OT stems from the historical differences between IT and OT. In Stouffer *et al.* (2023), OT is described as programmable systems and devices interacting with the physical environment. Examples of OT systems are process and discrete industries, energy production, healthcare and public health sector, chemical production and nuclear reactors (Stouffer *et al.*, 2023). This interaction with the physical world constitutes a crucial difference between IT and OT, and because of this interaction with the physical world, digitalized OT systems are often referred to as *cyber-physical systems* (Stouffer *et al.*, 2023). In the past, a classical OT system was built with specialized hardware. Control systems used proprietary operating systems and protocols for communication, and little communication occurred between the OT and IT systems (IEC, 2009). However, there has been a change in how OT systems are designed and operated. With the introduction of ethernet communication using internet protocols (IP), communication between machines has become almost plug-and-play. Further advancements in hardware to deal with increased demand for communication have, to an extent, removed the previous proprietary hardware with more standardized commercially of the shelf (COTS) technology (IEC, 2009), making communication between equipment from different vendors much more accessible. The motivation for this change in hardware and software is related to the Industry 4.0 model. The German Government first coined this term to increase industrial and economic growth (Corallo *et al.*, 2020; Sony and Naik, 2020). The increased interconnections between IT and OT opened up new business models, greater innovation and increased efficiency and effectiveness, allowing for predictive maintenance and higher output through gains in optimizing production by analyzing OT processes. However, this change from proprietary systems to an almost plug-and-play setup with COTS products and increased connections between IT and OT networks has opened multiple new attack vectors and vulnerabilities for OT systems.

Multiple research projects highlight that pure technical solutions are insufficient to mitigate the resulting risks. A state-of-the-art technical firewall does not suffice if the human firewall is flawed (Chowdhury *et al.*, 2019). Some form of balance between technocentric and sociocentric elements of security within the organization must be achieved (Sony and Naik, 2020; Malatji *et al.*, 2020).

This paper aims to uncover how Norwegian OT organizations prioritize these elements in their cybersecurity programs. A further aim is to uncover if there are peculiarities between IT and OT that should be taken into special consideration for organizations aiming to strengthen their cybersecurity standing. To this end, two data sources have been used, namely, seven semi-structured interviews with IT and OT staff from four different organizations; and data from a survey ($n = 34$) measuring the use of security controls deployed in their respective organizations. The study aims to contribute to answering the following overarching research question:

RQ1. What socio-technical challenges in improving cybersecurity in Operational Technology organizations do such organizations face?

The remainder of this paper is organized as follows: Section 2 reviews related work. Section 3 describes the used methodology. Section 4 presents our findings from both the interviews and the survey; challenges and areas to improve are discussed in Section 5. Finally, Section 6 summarizes our conclusions and outlines further research paths.

2. Related work

In (Whitman and Mattord, 2019), an information security program is defined as the entire set of activities, resources, personnel and technologies an organization uses to manage the risks to its information assets. A security program combines all aspects of managing security, from defining and communicating policies to implementing best industry practices, ongoing operation and auditing (IEC, 2009). Elements of a cybersecurity program are found in Whitman and Mattord (2019) and include but are not limited to: Policy, logical access control, risk management, physical security, audit trails and awareness and training; these elements relate to information security. In Stouffer *et al.* (2023), it is emphasized that OT systems have differences despite the convergence between IT and OT in the last decades and organizations should, therefore, initiate cybersecurity programs for OT. These should be consistent and integrated with existing IT cybersecurity programs and practices, and the specific requirements of OT should be considered.

2.1 Developing cybersecurity programs for OT organizations

Building a cybersecurity program is not a simple task, and it would be reasonable for organizations to search for sources of knowledge where such information could be easily obtained. Such sources can be found in legislation, standards, frameworks or guidelines. According to Djebbar and Nordström (2023), standards provide a structured approach to managing and accessing cybersecurity risks; therefore, standards are the primary source for security requirements that organizations use to reduce the likelihood and impact of a cyberattack. Cybersecurity standards are developed by large organizations like the International Electrotechnical Commission (IEC) or the International Society of Automation and standards produced by the different organizations can further be classified into international, regional and national standards. The most common standard for OT systems is the internationally recognized IEC 62443.

However, even though standards could provide organizations with a path to obtain the required knowledge to develop their cybersecurity program, some obstacles have been identified. In Leszczyna (2018a), 17 standards were found applicable in the context of cybersecurity of the smart grids, and this number is larger (Leszczyna, 2018b) when privacy is included in the context of smart grids, resulting in 36 standards applicable for the intended domain. This myriad of available material could be a hinderance for practitioners who, in a hectic work life, do not have time to read, understand and interpret which standard best fits their needs. However, does this mean that OT cybersecurity standards are not used?

Our previous work (Kannelønning and Katsikas, 2024) has shown that within the Norwegian Industry, only 32% of organizations have a cybersecurity program based on IEC 62443 or similar. In Wagner *et al.* (2020), the authors report that the usage of IEC 62443 in Small and Medium Enterprises is nonexistent and the usage in large organizations is at 25%. Several barriers to usage were found in the literature: the standards' size, voluminous scope and lack of practical advice are highlighted as such. With such a low application of OT cybersecurity standards, it is reasonable to suggest that specific OT security standards are not the source of knowledge one might hope for.

However, many IT-driven security standards, that organizations could use to increase their security, exist. One of the most used is ISO 27001, a standard for information security

covering some of the organization's OT sections, for example, regulation of employee's online behavior. According to Nüßer *et al.* (2017), 80% of German organizations follow the German BSI IT-Grundschutz, a German standard comparable with ISO 27001 and over 50% of German organizations are ISO 27001 certified (Mirtsch *et al.*, 2021). The ISO 27000 series is referred to in Malatji *et al.* (2020) as a compliance framework. If the organization complies with the standard and passes the audit, the organization will be ISO certified. One major drawback of such compliance standards is that an organization could achieve a certification level without necessarily having a stronger or more robust security posture (Malatji *et al.*, 2020; Øyvind Arntzen, 2022) than before the certification.

2.2 Socio-technical system

Cybersecurity is a complex topic, and a cybersecurity program consists not only of technical measures, but also of recovery plans and awareness training, to mention some elements. OT systems have changed drastically in the last decades after introducing the Industry 4.0 model. The motivation for Industry 4.0 is improved efficiency and growth through innovation and disruptive business models (Giannelli and Picone, 2022; Lezzi *et al.*, 2018). To achieve the goal of Industry 4.0, new technology must be introduced to OT systems, technology that will influence how work (tasks) is performed in organizations.

The proposed solution for cybersecurity in Industry 4.0, the shift in technology and how work is performed are found in socio-technical systems (STS) theory. STS was first coined by Emery and Trist (Fred *et al.*, 1960) and a classical STS combines the social and technical dimensions that are susceptible to their operating environments. A more concise description presented in (Malatji *et al.*, 2020) and accredited (Robert *et al.*, 1977; Walker *et al.*, 2007) is that *STS is made up of humans applying technology solutions to execute work activities through processes within a social structure (organization) to accomplish set goals*. References (Malatji *et al.*, 2020; Malatji *et al.*, 2019) investigate STS in the context of cybersecurity as a way forward to improve security. The premise for Malatji *et al.* (2020) to introduce STS in the context of cybersecurity is that humans are perceived as the biggest threat to an organization's cybersecurity. An organization's security level will have shortcomings if the social part is not considered, especially because technology improvements occur rapidly and the industry has focused on a successful technical deployment (Davies *et al.*, 2017). Many organizations, particularly large ones, do use socio-technical cybersecurity controls, including training programs. However, prior literature (see e.g. Christine and Thinyane, 2022), findings suggest that most organizations often prioritize technological solutions in cybersecurity while neglecting or underestimating socio-technical aspects such as human behavior, organizational culture and process integration, as well as their interaction with technology. This finding, focusing on organizations integrating IT and OT, has also been confirmed by our own research which, to the best of our knowledge, is the only one studying this topic in the context of organizations integrating IT and OT. In Table 1, a detailed list of social, technical and environmental elements has been mapped by Malatji *et al.* (2020); these STS elements are defined as the *STS framework* in the remainder of the text.

For Industry 4.0 to be successful, there should be equal consideration of the social and technical perspectives (Sony and Naik, 2020). The field of STS research in the context of Industry 4.0 has not received much attention from scholars, even though Industry 4.0 systems are socio-technical by nature (Sony and Naik, 2020; Davies *et al.*, 2017). Therefore, research into identifying if there is an imbalance between social and technical security efforts could be a viable way to improve cybersecurity in this domain.

STS dimension	Capability domain	STS security controls	Ranking Usage (1-24)	Ranking Importance (1-24)	Score Usage	Score Importance	Delta ranking	Delta score
			A	B	C	D	E	F
Social	Organizational structure (Functions)	Communication						
		Cybersecurity change management activities						
		Cybersecurity governance						
		Cybersecurity team training (Specific Cybersecurity OT training)	23	17	71	135	6	64
		Human resources onboarding activities of new employees						
		HR employee management during employment						
		Other physical security activities (Fences and controlled entrances)	4	7	134	147	3	13
		Physical access controls						
		Frequent user awareness training						
		User awareness campaigns						
		User identity awareness						
		Continuous self-learning by cybersecurity team						
		Cybersecurity operations center management						
		Cybersecurity team management						
		Organizational structure impact on cybersecurity						
		Organizational culture-driven cybersecurity activities						
		Phishing campaigns						
		Understanding information security standards						
		Employees off-boarding and rights revoked	9	11	122	143	2	21
Technical	Technology (Tools & resources)	Anti malware						
		Antivirus software (for OT)	11	22	111	127	11	16
		Firewall						
		Host-based intrusion prevention system						
		User awareness policy						
		Active directory						
		Application layer filtering						
		Assets management policy (OT installed based)	10	6	112	148	4	36
		Back-up-as-a-service (Back up of critical SW w/o as-a-service)	1	1	146	162	0	16
		Cloud security policy						
		Cybersecurity policy						
		Cybersecurity standards						
		Data breach policy						
		E-mail security						
		Honeypot						
		Network authentication controls (MFA for remote OT connections)	13	9	109	144	4	35
		Password policy (PLCs are password protected)	24	24	65	116	0	51
		Steganography						
	Work activities (Tasks)	Cyberrisk assessments and analysis (internal and external)	17	16	98	135	1	37
		Disaster recovery and business continuity (Continuity plans for OT)	16	15	102	140	1	38
		Systems access control (Engineering Workstations unique log-in)	8	8	123	144	0	21
		Systems hardening						
		Video surveillance						
		Cybersecurity audit (internal and external)						
		Data encryption						
		Data leakage protection						
		Documentation of cybersecurity practices						
		Identity and access management (Role based Privileges and access rights)	3	12	135	143	9	8
		Incident response and management						
		Network segmentation (IT/OT network segmentation)	6	3	131	154	3	23
		Network traffic monitoring (IDS for OT)	20	23	88	126	3	38
		Patching and systems security updates	18	19	94	131	1	37
		Penetration testing (red team exercise)						
		Virtual private network configuration						
		Vulnerability scans and assessments (Vulnerability management)	22	21	79	129	1	50
		Remote connections to OT are known	2	2	140	158	0	18
		Overview of, and security on OT wireless	7	10	126	144	3	18
		Network Architecture documentation	12	5	109	149	7	40
		HW redundancy of critical components	14	18	108	133	4	25
		Check of external devices before connection to OT	15	14	104	141	1	37
		Specific OT response and recovery plans	21	13	88	142	8	54
		Unused ports are disabled	19	20	90	130	1	40

Table 1. Findings of the survey

2.3 Human cybersecure behavior

Organizations implement cybersecurity countermeasures (policies, procedures, technical security controls) to decrease the likelihood of successful cyberattacks. A prerequisite for successful avoidance of cyberattacks is how the staff of the organization behave. Research consistently highlights that human behavior is a major factor in cybersecurity compliance issues, often surpassing technological vulnerabilities. Some recent sources (and references therein) that support the argument that cybersecurity compliance problems are frequently caused by human behaviors rather than purely technical shortcomings are:

- Khadka and Ullah (2025) emphasizes that cybersecurity is not just a technological challenge but is deeply influenced by human decision-making and organizational culture. It argues that compliance failures often stem from behavioral gaps, such as poor security awareness and resistance to security policies.
- Sulaiman *et al.* (2022) found that despite advanced security systems, organizations remain vulnerable due to noncompliant human behavior. The study is one of many that identify employees as the "weakest link" in cybersecurity, with violations often occurring due to negligence, lack of training or intentional disregard for security protocols.
- Delso-Vicente *et al.* (2025) highlight that organizational culture, leadership and individual attitudes significantly shape compliance behaviors. It suggests that compliance strategies should integrate behavioral motivators alongside technical solutions to effectively reduce security risks.

Human cybersecure behavior, behavior that follows the prescribed policies and procedures of what to do and what not to do, is crucial for the success of keeping the organization secure. Even though employees are required to follow cybersecurity policies and rules as they are non-negotiable enterprise level policies, the reality is different. Factors such as employee attitudes toward compliance, awareness of the implications of noncompliance, and familiarity with security protocols profoundly shape workplace behaviors that are not necessarily compliant with policies (Khadka and Ullah, 2025). has found that perceived effectiveness of security measures, top management support and organizational culture are pivotal in shaping such behaviors. One of the findings of Khadka and Ullah (2025) is that strategies that combine intrinsic motivators, such as personal responsibility, with extrinsic incentives, like rewards and enforcement, are identified as the most effective for shaping compliance behaviors.

Mitigating malicious intentions is difficult for any organization. However, for some staff of the organizations, these organizational prescriptions may appear overcomplicated and burdensome and as a result, cybersecurity is not only threatened by malicious intentions but also by *nonmalicious*, *nonsecure* behavior (Chowdhury *et al.*, 2019). Examples of nonmalicious nonsecure behavior from security personnel include haste in security rollouts, leading to inadequate system security or poor patch management, while for general users in the organization, nonmalicious behavior might be leaving the workstation logged in or using weak passwords (Chowdhury *et al.*, 2019).

Noncompliant behavior may stem from many different avenues. In their literature review, the authors of Chowdhury *et al.* (2019) investigate time pressure as a factor in such behavior. Time pressure refers to "objective or subjective perceived limitation of the available time needed to consider information or to take a decision" (Jean-Christophe and Pochwatko, 2008). Some of the work reviewed in Chowdhury *et al.* (2019) suggests that time pressure leads users to disregard security prompts, for example, disregard browser warnings, overlook

security cues regarding wireless connections or share workstation user logins because they are sometimes "quite busy with other things." Users who operate in a sustained time-pressure environment might show indifference toward security if security practitioners fail to highlight the importance of cybersecurity. Such indifference could lead to a culture of nonsecure behavior, like finding nonsecure workarounds, that is, *shadow security* (Chowdhury *et al.*, 2019).

The importance of communicating to the organization how important it is to follow the security policy of the organization is also highlighted by Chowdhury *et al.* (2019), Herath and Rao (2009) and Hwang *et al.* (2017). If employees do not understand that their individual contribution to security is important for the organization's overall security (Herath and Rao, 2009), noncompliant peer behavior could become a security risk. Peer behavior is a key element for compliant behavior, as employees follow the norms of their peers. If one coworker does follow the prescriptions of correct behavior, it is likely that peers may act similarly in not following the organization's policy (Hwang *et al.*, 2017; Alzahrani, 2021). Hwang *et al.* (2017) found that employees' intention to comply is negatively affected by noncompliance by their peers. To mitigate noncompliant peer behavior, it is important to investigate the organization's cybersecurity culture, as the literature states that peer and policy-compliant behavior is only achievable when there is a positive cybersecurity culture in the organization (Alzahrani, 2021; Parsons *et al.*, 2015; Reeves *et al.*, 2020). Building and maintaining a positive cybersecurity culture is a task assigned to management.

There are many reasons why people do not comply with specified policies. According to Bada *et al.* (2019), the two most compelling reasons are that people are unaware of (or do not perceive) the risks or do not know (or fully understand) what the correct behavior is. This is referred to as risk perception, and in a condensed form, it refers to how humans understand the risks they face. According to Reeves *et al.* (2020), risk perception can be explained by two factors: familiarity and dread. Dread refers to the extent to which someone is scared, troubled or generally retracts away from the risk at the level of gut feeling, while familiarity refers to the extent to which someone feels they have the knowledge to understand the risk and to what extent they can control the outcome. Risk perception is important because overestimating the risk can stifle users from adapting IT solutions, while underestimating the risk can lead to insecure behavior (Huang *et al.*, 2011; Parsons *et al.*, 2010). The main influences on individual behavior in cybersecurity are the individual's knowledge, skills and understanding of cybersecurity in combination with past experiences, perceptions, attitudes and beliefs (Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015) Of these, personal motivation and ability are the two most important.

The remedy for increasing employees' knowledge levels is proposed to be found in cybersecurity awareness campaigns. For such campaigns to be successful, three key foundations must be established. First, people must admit that the information is relevant. Second, understand how they should act and third, be willing to do this while many other pressing factors require their attention (Rogers, 1985; Witte, 1993). Awareness and training campaigns provide the organization with needed information on cyber risks and the importance of compliant behavior. But does successful fulfillment of the included test at the end of the training session guarantee compliant behavior? Will knowing the responses to a test translate into behavior? According to Bada *et al.* (2019), the fact is that today's security awareness trainings is not working as expected. It is only natural when faced with ambiguous warnings and complicated advice that many are tempted to abandon all efforts for protection and not worry about any danger. Intimidating security warnings increases stress to such an extent that the individual may even deny the need for any security decision (Bada *et al.*, 2019). Combined with security procedures that feel like obstacles for the primary task may

lead to "security fatigue," a feeling that could lead to the abandonment of security altogether (Bada *et al.*, 2019).

2.4 Research questions

Reviewing the work presented in this section leads to defining the research questions for this study. The entire set of activities, resources, personnel and technologies an organization deploys to reduce risk to its information assets is defined as its cybersecurity program (Whitman and Mattord, 2019). However, defining the best way, a blueprint, to organize this work is not information easily obtained in reference work like cybersecurity standards. Previous research found that few organizations rely on cybersecurity standards for OT systems (Kannelønning and Katsikas, 2024). The voluminous size and lack of practical advice were identified as barriers to the usage of cybersecurity standards.

According to Evripidou *et al.* (2023), cybersecurity research for OT systems is just in its infancy, and research into the cybersecurity of OT systems is scarce compared to IT systems. With current knowledge stemming from research on IT systems and the highlighted differences regarding the cybersecurity of IT and OT systems found in Stouffer *et al.* (2023), IEC (2009) and Lezzi *et al.* (2018), it is interesting to examine if there are deviations between IT and OT systems and investigate how this affects the overall goal of cybersecurity to reduce the risk of unwanted events. Furthermore, Malatji *et al.* (2020), Malatji *et al.* (2019) and Al Sabbagh and Kowalski (2012) argue that an organization's cybersecurity efforts should balance the socio- and the technical dimensions to achieve the highest possible outcome. In light of the statement in Sony and Naik (2020) that OT systems are socio-technical by nature but have still not received the proper attention of scholars, it is valuable to uncover new information as to how organizations organize and prioritize their OT cybersecurity efforts, particularly when it comes to balancing its technical and social dimensions, leading to the first research question:

RQ2. How do OT organizations prioritize the technical and social dimensions in cybersecurity programs and what, if any, differences exist with IT security?

Humans are attributed to be the weakest link in organizations' cybersecurity defense (Kruger *et al.*, 2020). Statements similar to the one in Chowdhury *et al.* (2019) stating that "the human firewall is flawed" are commonplace. It is unclear whether human error, inadequate implementation of technical security controls or poorly executed awareness campaigns (Bada *et al.*, 2019) are the obstacles that organizations face in achieving improved cybersecurity results. Therefore, the second research question for this study is defined as follows:

RQ3. What socio-technical challenges must OT organizations overcome to improve their OT cybersecurity?

3. Methodology

Cybersecurity research and results are influenced by the culture in which the research is conducted. According to Da Veiga (2016), culture can be classified into four levels: personal, organizational, national and international cybersecurity culture. This study is limited to the Norwegian industry, and the scope is, therefore, at the national cybersecurity cultural level. By focusing on one cultural level, the results benefit from removing cultural differences, for example, trust or legislation, thereby improving the accuracy of comparing the results or statements between respondents; this strengthens internal validity and enables clearer

identification of socio-technical dynamics. Nevertheless, we emphasize that Norway's OT sector shares structural and technological characteristics with other advanced industrial economies, making the findings potentially transferable. Note that our contribution lies in identifying socio-technical gaps and governance challenges that may be common across OT organizations globally, while acknowledging the contextual limitations.

This study was intended in its early planning phase to rely on one source of data: qualitative data obtained through interviews. It should be noted that the industrial market integrating IT and OT is relatively small in Norway. This research has focused on OT organizations that are asset owners, that is, having their own production site, thus narrowing the target market further. An indication that the market is small is also highlighted in the survey recruitments process, where only 81 potential participants were identified, a process that was based on referrals from about 15 employees from Norway's largest supplier to this market. This means that the study engaged a good portion of the defined market. The precise scoping and small Norwegian market resulted in fewer interviews than first intended. To mitigate the limitation of the few interviews, it was decided to expand the data collection to include survey data from the same demographic area.

Qualitative methods explore context, meaning and experiences, while quantitative methods provide measurable, statistical validation. Together, they offer a balanced view of complex issues (Rothenberg-Elder, 2023). Quali-quantitative research allows for deep exploration of themes while also testing hypotheses with numerical data, making it ideal for interdisciplinary studies [1].

The appropriate sample size in qualitative research is influenced by several factors, including the nature of the research question, the chosen methodology and the concept of saturation. Originally introduced "theoretical saturation," this concept refers to the point at which additional data collection yields no new properties or theoretical insights regarding the emerging grounded theory. As explained in Bryant and Charmaz (2007), theoretical saturation occurs when all relevant issues have been thoroughly explored and the conceptual categories are sufficiently developed, resulting in a comprehensive and well-grounded theory.

In contemporary qualitative research, saturation is more commonly referred to as "data saturation" or "thematic saturation" (Bryant and Charmaz, 2007). This broader interpretation shifts the focus from theory development to determining sample adequacy. In this context, saturation denotes the stage at which no new themes or insights emerge from the data and subsequent interviews begin to replicate previously identified patterns, indicating that further data collection is unlikely to yield additional value (Francis *et al.*, 2010).

Unlike quantitative studies, which emphasize breadth and statistical generalizability, qualitative research prioritizes depth and contextual richness. Consequently, sample sizes tend to be smaller. A literature review cited in Hennink and Kaiser (2022) found that saturation was typically achieved within 9–17 interviews, particularly in studies with a relatively homogenous population and narrowly defined objectives; conditions that align with our study design. In our case, thematic saturation was reached, as no new themes emerged during the final interviews. Moreover, responses across participating organizations demonstrated strong convergence, reinforcing the adequacy of our sample and the robustness of our findings.

Interviews are well suited for understanding the "how" and "why" of a particular contemporary event (Yin, 2018). In our case, "how" and "why" organizations prioritize cybersecurity controls and make cybersecurity decisions. Note that results from interviews, especially with few interviews conducted, cannot be generalizable to populations or universes but can contribute to expanding and generalizing theories (analytic generalization)

rather than aiming to extrapolate probabilities (statistical generalization). The goal of a single-case study is to do a "generalizing" and not a "particularizing" analysis (Yin, 2018).

On the other hand, survey data provide quantitative data from a larger population within the same demographic on what security controls organizations prioritize and implement within their cybersecurity programs. The benefit of using two data sources arrives when the results converge, meaning multiple sources of evidence provide multiple measures of the same phenomenon (Yin, 2018). By developing converging evidence, data triangulation helps strengthen the validity of the case study (Yin, 2018).

3.1 Interviews

During the spring of 2023, seven semi-structured interviews were conducted with employees from the Norwegian Industry. An interview guide, available at **url blinded for review**, was developed. This approach shaped the direction of the recorded interview; however, it did not mandate strict adherence to the interview guide or a step-by-step format (Yin, 2018). The interview guide developed for the interviews was pretested with members of academia and participants from the Norwegian Industry, before the Norwegian Agency for Shared Services in Education and Research (SIKT) approved it as compliant with the data protection legislation.

Four different organizations were recruited to participate, with two participants from each organization, the leader of IT and the leader of OT. The decision to interview IT and OT was made to understand how the respective organizations view, prioritize and execute cybersecurity-related issues and to capture the differences within the respective IT and OT disciplines. One of the four organizations participated with one person; however, that participant was responsible for both OT and IT. All participants have more than 20 years of experience within their respective fields of expertise. Moreover, all participants hold cybersecurity or OT operational responsibility within their department. One organization operates within discrete manufacturing, producing finalized end-products, one operates within food and beverage and the last two operate within process automation. Three are classified as large organizations with more than 1000 employees; these are also multinational. The last operated only in Norway and had, at the time of the interview, around 150 employees. The commonality between the organizations is that all are defined as asset owners, that is, owners of a production plant or facility. The decision to include one organization substantially smaller than the other three was so as to get a feeling or indication regarding differences between large and medium enterprises. Including one organization smaller also fits well with the demographic from the survey. In the survey, the classification of the organizations' size follows guidelines from the EU NIS2 Directive, with the following distribution: 0–50 employees: three (8%), 51–250 employees: 11 (29%) and 251 and more: 24 (63%).

The interview covered three thematic topics. The first topic in the interview investigated the usage of security standards. The second and third topics focused on cybersecurity programs and motivation or personal drivers for acting in accordance with the organization's prescribed policies, respectively. The section on cybersecurity programs aimed to investigate how organizations build up, maintain and prioritize their cybersecurity efforts to be more cybersecure. The section regarding motivation for acting compliant stems from the statement that humans are deemed the weakest link and therefore, discovering what might be barriers to compliant behavior is essential to understand if future cybersecurity levels are to be improved.

Section 1 of the interviews revolved around the topic of the interviewee's organization's cybersecurity program, starting wide by asking the participants, "How do you define

cybersecurity?" As the interview progressed, the questions became increasingly more focused. After the participants had defined what cybersecurity meant to them and their role, a simplified description of STS (Malatji *et al.*, 2020) was introduced. The participant was invited to describe how this fitted into their perceived view of cybersecurity and comment on whether this was a reasonable way to categorize cybersecurity. The interview section concluded with questions regarding the strengths and weaknesses of the STS model and cybersecurity in general.

An excerpt of some of the questions can be found below.

Cybersecurity program:

- When thinking of cybersecurity, how would you describe it and what are the components of cybersecurity?
- With your previous answer in mind, what are the most important components? (which is the weakest)
- How do you prioritize your cybersecurity efforts in your organization?

Motivation for compliant behavior:

- Could you describe your organization's cybersecurity culture?
- How do you believe peer behavior is influencing staff in your organization?
- In your opinion, to what degree do workarounds (noncompliant behavior) exist and what might be the cause of such workarounds?

All interviews were conducted remotely during the spring of 2023. Verbatim transcriptions of the interviews were made before the analysis commenced. The interviews were analyzed using template analysis. The term "template analysis" does not describe a single, clearly delineated method but instead refers to a varied but related group of techniques (Nigel King, 2004). Template analysis is a form of thematic analysis that emphasizes the use of hierarchical coding but balances a relatively high degree of structure in analyzing textual data with the flexibility to adapt it to the needs of a particular study (Brooks *et al.*, 2015). Template analysis shares with Braun and Clarke's (Braun and Clarke, 2006) approach the flexibility and focus on developing a hierarchical code. However, one particular difference is the use of an initial template. A distinctive aspect of template analysis is its reliance o*n a priori* themes, enabling researchers to outline certain themes before the analysis process begins (Braun and Clarke, 2006). Often, the best starting point for creating an initial template is the interview guide – the set of question areas, probes and prompts used by the interviewer (Nigel King, 2004). Consequently, as presented in Figure 1, the center pie chart represents the initial template derived from the interview guide, while the left and right charts, indicated with broad arrows, present the second hierarchical step. Template analysis is very well suited when studying different perspectives of different groups within an organizational context, for example, different professions working in a collaborative setting (Nigel King, 2004); in our case, IT and OT professionals addressing their organization's cybersecurity challenges.

The findings of the interviews are compared to the ranking resulting from the (larger) survey population to understand the "why" and "how" organizations prioritize their cybersecurity efforts.

3.2 Survey

The survey was also performed in 2023 among 34 organizations operating within the Norwegian Industry. The questions were all of the closed type and they were developed by leveraging the NIST special publication "Guide to Operational Technology," SP 800 - 82r3.

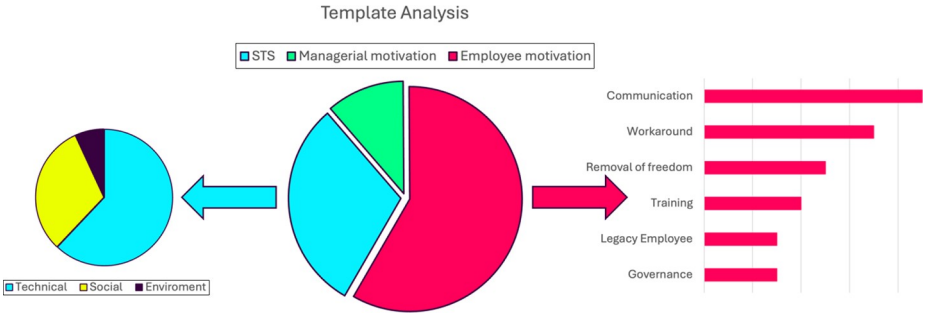

Figure 1. Prevalent themes in interviews resulting from the template analysis. The center pie chart represents the first analysis of the *priori* codes, while the left and right diagrams present the hierarchical development of the analysis

The security controls were grouped and classified in agreement with the NIST Cybersecurity Framework v1.1 (NIST CSF Version, 2018) core functions [2]: identify, protect, detect, respond and recover. The full questionnaire can be found at **url blinded for review**. In Kannelønning and Katsikas (2024), an extended and detailed description of the survey instrument, sample selection, recruitment and distribution and data quality assurance and analysis can be found; these are not repeated here, in the interest of saving space. Even though some primary results from the survey were reported in Kannelønning and Katsikas (2024), the data presented and analyzed in the present work have not been reported before.

In this work we report on the numerical ranking (1–24) of the security controls, the average score of usage and importance and the delta score of usage and importance and the delta ranking of usage and importance. Herein, the security controls have been mapped and categorized according to the STS framework proposed in Malatji *et al.* (2020). The survey results were fully analyzed statistically in Kannelønning and Katsikas (2024), showing a satisfactory result for Cronbach's alpha and normality of the data set.

4. Findings

4.1 Interview findings

In Figure 1, the center pie chart represents the first hierarchy of the analysis. This is further analyzed in terms of STS elements, where there is a clear overweight of technical elements from the interviews. The group termed "employee motivation" is further coded, with the following codes receiving the broadest consensus: Communication; workaround; removal of freedom; training; legacy employee; and governance. These will be discussed in the sequel. Even though the themes that were unveiled by the template analysis enjoy the broadest consensus by the participants, this does not infer that the statements or topics have equal prevalence within each organization. When the findings from the two data sources coincide, this provides convergent evidence that solidifies the findings.

Observing and analyzing the transcripts quite immediately showed trends in the responses. Naturally, everyone's response has variances depending on experience and type of organization. However, two things stood out. First, the responses from IT and OT personnel vary substantially regarding what the participants perceive as included in cybersecurity. IT personnel elaborate substantially, while OT personnel have not given the subject much thought. Or at least they do not express themselves with many words regarding their thoughts

about "What is cybersecurity." The second impression at the start of the analysis is that responses across organizations have similarities. This is true for both IT and OT participants.

The most noteworthy difference between IT and OT, from a high-altitude perspective, is that OT personnel view cybersecurity solely as a technical challenge. To them, cybersecurity is a technical problem, solved with technology and solved preferably with technology outside their domain of responsibility. In contrast, IT participants include all or at least most of the aspects found in the literature (IEC, 2009; Whitman and Mattord, 2019), spanning from governance documents, crisis management, onboarding and offboarding, fences and controlled gates and culture and awareness programs, to mention some areas. Even though the responses from IT participants would include more elements than just technology, all participants agree that the cornerstone of cybersecurity starts with technology. Without technology, there would be little or no production. Hence, technology needs to be part of the organization and will also be the most important element of cybersecurity. Furthermore, all participants agreed that the most significant threat is human noncompliant behavior. These findings confirm findings already known from the literature.

Not surprisingly, OT personnel did not have much input into how the STS framework would fit in cybersecurity, being firm as to "technology equals cybersecurity." IT personnel provide a more nuanced response and could see a benefit, if not to apply the STS framework itself, to see the value in measuring if there is a gap between the social and the technical part. Given the consensus of responses that technology is the primary driver for cybersecurity and humans are the weakest link, such a framework could provide exciting findings.

As with many parts of an organization, a budget is required to continuously improve existing cybersecurity initiatives or replace hardware with new, faster and better technology. Without funding, limited efforts could be implemented. Several questions were asked, but the overarching topic was "what motivates higher management to make cybersecurity decisions." Not surprisingly, personnel from OT kept this section short, with very few opinions and the reason for the short replies might be OT personnel's limited interaction with higher management (Evripidou *et al.*, 2023). On the other end of the scale are the IT personnel in this study. All are responsible for cybersecurity and frequently interact with and report to higher management. Their responses could be summed up and distilled quite succinctly: *Senior management understands risk. They understand the concepts of risk, risk mitigation and risk transfer. If you can present risk in monetary numbers, even better. For senior management, it is as simple as an equation: if the cost of the risk is higher than the cost of the remedy, then you will get the required funding.*

Drilling further into how organizations can be more cybersecure, the final thematic section of the interview concentrated on nonmalicious, noncompliant behavior and how this can be avoided. Several themes emerged through the analysis, but the topics with the broadest consensus among all participants were the removal of employee freedom; communication; and workarounds.

With the introduction of Industry 4.0, previously isolated systems are susceptible to more cybersecurity risks than in the past. All participants agree that this new "world" has changed the everyday work within OT. Changes can be challenging in any aspect of life, and age is generally not a catalyst for adaptation to change. Change is not easy when having a large pool of OT legacy staff members, a term used by one of the participants who stated, "I am 51 and am the youngest working with OT." The most consequential change for OT personnel is removing the freedom to operate that they had in the past. This removal of freedom manifests itself in many ways through the interviews, but some of the recurring items are the inability to download software tools needed and difficulty in making remote connections to production sites. "It is just so much harder now than it used to be. I cannot use tools other

than those approved by IT. If they do not trust me to download the tools that I need, I end up feeling like my contribution to security is zero. I think many just turn their brain off because they do not feel any ownership of this thing called cybersecurity." One interesting finding is that IT participants, who are all responsible for cybersecurity and are also part of deciding the policies, guidelines and so forth, agree that having a paternalistic cybersecurity program is not a viable governance structure. Having a governance structure that inhibits employees from having autonomy to complete their tasks is not a viable solution. Still, this consensus by the IT participants is in dire conflict with what OT personnel report, who feel a substantial removal of freedom is evoked upon them.

Following this, actual or perceived removal of freedom follows the topic of communication. Communication is a topic frequently mentioned on both sides of the aisle. The communication of cybersecurity and the risks affiliated with cybersecurity is a task residing within the IT department. Several IT staff members say that communication of risk is their most pressing matter: "I cannot be security for the whole organization. As a single person, it is just not viable. Therefore, I focus time and effort on communicating risk to the organization by making cybersecurity a business enabler. I want the employees to understand that security is paramount for continuous production and that they need to be part of the team." Even though communication is an essential subject for IT, participants also acknowledge that communication is difficult.

According to the OT interviewees, the recipients of cybersecurity-related communication, the lack of an understanding of *why* security controls are necessary for security, is a pathway for noncompliant behavior. One participant exemplifies this lack of understanding *why*, with the requirement of using two-factor authentication for login on workstations. "Everyone in my team understands why we use two-factor in our bank. Nobody wants to lose their money, but they do not grasp why they need it to log into a workstation." Furthermore, the OT participants also expressed that the communication did not resonate with the recipients working within OT. "We are constantly trained through awareness campaigns not to click the link in an email, but simultaneously management sends out the paycheck on a link. People are confused." Another example of a communication barrier is language, either stemming from training in a non-native language or using cybersecurity-special terminology. General cybersecurity awareness training is reported to have a sufficiently high frequency; however, "The training is probably well made, and with good intention, but it includes difficult words that might be easy to understand when cybersecurity is your primary occupation, but it just goes way above the head on the workers maintaining our production sites. Those small misses deteriorate the workforce's morale and reduce efforts coming from IT." These exemplified communication gaps between the recipient and the sender lead to workarounds, the last of the main findings found in the interviews.

Almost all participants acknowledge that workarounds could exist. The IT participants do not, however, believe that there is a widespread use of workarounds in the OT environment. The story pivots drastically when the response from OT is analyzed. Several entertaining stories emerge as examples of workarounds, and one is worth highlighting. One of the organizations has previously been affected by a severe cyber-attack and has therefore inflicted strict rules for IT and OT. One mandatory security control implemented by IT is automatically locking all PCs after a very short time, approximately 1 min. This resulted in substantial additional daily logins for users. To such a high degree, it became an annoyance and a burden. The solution came from a local IT professional who is part of the team responsible for IT security. This local IT person found a software, legally downloaded from the organization's software library, that moves the mouse ever so slightly every minute. The result at the time of the interview was that every employee in that location had PCs that never

automatically locked down, not even at lunch, according to the OT participant. When asked, the chief information security officer (CISO) of that organization did not know of or believed that any workaround existed in their organization. "The way I see it, our organization should not have any workarounds. We have strict but reasonable rules for our employees." This anecdotal example does not prove that participants from IT are blind to the fact that workarounds could exist. As one CISO pointed out, "We know that the workload becomes tougher with security. Things do take longer if we are to be secure, but this needs to be addressed by the employees in their yearly review meeting with their leader. Otherwise, we as CISOs cannot adjust our security demands, and there should be a match between workload and security."

4.2 Survey findings

With the survey data regarding the usage of cybersecurity controls, it is possible to identify how and what security controls are prioritized within the Norwegian Industry and if there are any STS gaps. One important issue to address is that participants in the survey ($n = 34$) did not have a say in what security controls were included in the survey, and no free text area was provided to include additional security controls. In the context of STS, there is a skewed selection of security controls in favor of technology, meaning more security controls are classified in the technical dimension than in the social dimension in the survey. Technical skewness resonates well with findings from Malatji *et al.* (2019) investigating security frameworks, as (Malatji *et al.*, 2019) provides results showing that no cybersecurity framework achieved a full score on the social part, although all frameworks did achieve fulfillment on the technical part. Given that the measurement scale was developed after Stouffer *et al.* (2023), it is reasonable that the measurement scale in the survey includes a larger number of technical security controls. The survey included three security controls related to the social dimension and 21 security controls mapped onto the technical dimension. In total, 24 security controls were included in the survey.

Table 1 depicts the survey results categorized according to the different STS elements as in [6]. Highlighted in *bold* are STS elements from this survey that have not been reported in [6]. Terms in parentheses were used in the survey to describe each corresponding OT security control.

Columns A to F depict the results from the survey. Columns A and B depict the ranking of each security control in the range (Stouffer *et al.*, 2023; IEC, 2009; Corallo *et al.*, 2020; Sony and Naik, 2020; Chowdhury *et al.*, 2019; Malatji *et al.*, 2020; Whitman and Mattord, 2019; Djebbar and Nordström, 2023; Leszczyna, 2018a; Leszczyna, 2018b; Kannelønning and Katsikas, 2024; Wagner *et al.*, 2020; Nüßer *et al.*, 2017; Mirtsch *et al.*, 2021; Øyvind Arntzen, 2022; Giannelli and Picone, 2022; Lezzi *et al.*, 2018; Fred *et al.*, 1960; Robert *et al.*, 1977; Walker *et al.*, 2007; Malatji *et al.*, 2019; Davies *et al.*, 2017; Christine and Thinyane, 2022; Khadka and Ullah, 2025). The ranking is based on the average usage and importance score of the security control. Columns C and D depict the average score of each security control and columns E and F depict the delta (absolute difference) between usage and importance in ranking and average score, respectively.

The STS model used in Malatji *et al.* (2020) consists of two more social dimensions, namely, the capability domain "actors or people" and the "environmental" section; these do not appear in Table 1 because no security controls in these two domains were included in the survey.

Analyzing the data by rank based on the usage and importance score highlights some interesting findings. Obviously, the highest and lowest-ranking security controls are of some interest, but analyzing the delta between usage and importance is more interesting. In

Kannelønning and Katsikas (2024), one of the investigated hypotheses was that individuals would, in a cybersecurity context, do what they think is important, that is, it was expected that if the participant believed risk assessments were an integral and important security control, then risk assessments should be performed in the organization. This did not pan out to be true, with a possible explanation in the distance between one individual's belief and an organization's actions. It is easy to have an opinion as an individual, but it is something else to turn one's opinion into concrete actions in an organization. Time constraints, monetary constraints and management risk appetite are potential barriers. Turning the hypothesis upside down, proposing that an organization at least should *not* do what is not perceived as important, reveals some exciting findings in column E, depicting the delta between ranking of usage and importance. The four highest differences between usage and importance are highlighted. *Antivirus for OT* and *Identity and Access Management (Role-based Privileges and Access Rights)* are ranked with a high degree of usage, ranked 11th and 3rd, but are not ranked highly in importance, specifically 22nd and 12th, respectively. It is especially interesting that *Role-based Privileges and access rights* are widely used (3rd) but not perceived as important.

Similarly, column F presents the delta in the average score of each security control to identify gaps in what is important but still not used. The highest difference in score is found in the social dimension under *Cybersecurity team training* (*Specific cybersecurity OT training)*; few receive such training, but participants do think specific OT training is important. Similarly, specific *OT response and recovery plans* are perceived by participants as important but are not used to a large extent.

An interesting observation is that both *Password policies on Programmable Logic Controllers* and *vulnerability management* have a high delta in score but not in ranking. This indicates that scores and rankings must be combined to identify gaps.

In Lars Halvdan Flå *et al.* (2024) the authors report on the findings from interviews with ten organizations, all asset owners and all within the Norwegian Industry. The same criteria were used for participating in this study. The authors of Lars Halvdan Flå *et al.* (2024) identified seven cybersecurity challenge areas for asset owners through their interviews. Two of the challenges that are especially relevant to this work are *establishing asset inventory* and *vulnerability context*.

Several participants in Lars Halvdan Flå *et al.* (2024) highlighted the importance of an asset inventory while acknowledging the challenges of establishing, maintaining and updating it. Participants in our survey rank the usage of an asset inventory in the 10th place and on the 6th place on importance, which means that they rank the importance of asset inventory management in the top quarter of security controls. Related to the challenge of keeping the assets updated (Lars Halvdan Flå *et al.*, 2024), highlights that many reportedly use automated solutions like intrusion detection systems (IDS) to compile and update their asset inventory. Looking at our survey results, the usage and importance of IDS are very low, respectively, 20th for usage and 23rd for importance. IDS is ranked second to last on importance in this study. This might suggest that the organizations participating in this survey could have difficulties upholding an updated asset inventory database if no other automated system is used to collect asset information.

Challenges in asset management and the consequences of maintaining an outdated system can have far-reaching ripple effects, particularly if the asset inventory database serves as the primary data source for the vulnerability management system; a lack of up-to-date asset inventory could lead to incomplete vulnerability information. Results from this survey suggest that the primary challenge is not the presence of incomplete vulnerability information but rather the absence of vulnerability information altogether. The usage of

vulnerability management systems is ranked in the 22nd place and the importance of vulnerability management is in the 21st place, right at the bottom for both usage and importance.

An organization's knowledge regarding its installed base and vulnerabilities affects the decision to perform patching to its system. To understand the impact of a vulnerability, the context of the vulnerability must be established. The vulnerability context is highlighted in Lars Halvdan Flå *et al.* (2024) as one of the seven main challenges for OT organizations. The vulnerability context influences the need for expediting patches, for example, a system located outside of all critical business activities and with no outside connections might have a lower urgency than a highly networked component crucial for operations. Some of this information stems from asset management systems and some from vulnerability management systems. Independent of how and where the information stems from, it is advantageous to have such information to understand the vulnerability context leading up to the decision to install patches.

Patching is well known as a remedy for vulnerabilities and IT professionals have known for decades that this can be an incredibly effective mitigation measure (Souppaya *et al.*, 2018). Even though several high-profile cyber-attacks, such as NotPetya and the Equifax data breach, have been attributed to lack of or delayed patching (Thakur, 2024), it is still difficult for organizations to decide how, when and what to patch. Security must balance mission impact and business objectives and determine risk tolerance (Souppaya *et al.*, 2018). This is especially true for OT systems that strongly emphasize availability. Although there is consensus in literature and with proven consequential impact following inadequate patching from cyber-attacks like NotPetya and Equifax, it might be reasonable to suggest that patching should, if not often used, at least be a highly important security control. This is not confirmed by the data collected in this survey: knowledge about available patches and a process for patching is not used much (18th place) and participants do not think it is important either (19th place).

5. Challenges and areas to improve

Perhaps not surprisingly, the responses from IT are more elaborate and holistic than the responses from OT. A plausible reason could stem from the realization that IT is often responsible for both IT and OT security, at least for any connections between the outside world and OT. Interview participants confirm that the responsibility for security resides with the IT department, but there are somewhat conflicting statements about *who* is responsible. From an IT perspective, everyone is responsible for security, even though the responsibility is eventually placed within IT. In contrast, the OT perspective is highlighted by the synopsis that cybersecurity is preferably something solved with technology and with technology outside the OT domain.

Receiving more elaborate and holistic responses from IT is also in accordance with previous research (Kannelønning and Katsikas, 2024) where familiarity and knowledge regarding security standards were researched. IT personnel have a far superior knowledge of standards and standards are, in essence, holistic, although no standards or frameworks have been found to have a socio-technical balance (Malatji *et al.*, 2019). Results from the interviews regarding RQ1 and how OT organizations prioritize their cybersecurity efforts unfortunately do not provide, in a distilled version, more insight than the acknowledgment that IT governs cybersecurity in the organizations and that there is a gap between IT and OT regarding how cybersecurity is perceived and what it consists of.

Although the interviews did not provide great in-depth knowledge of how OT prioritizes cybersecurity, the survey could give noteworthy insights because all respondents were OT

personnel. Following the finding that organizations deploy and use security controls that participants do not find important, *Antivirus for OT* and *Identity and Access Management (Role-based Privileges and Access Rights)* are the two security controls with the highest deltas; they are highly used but not deemed important. For Role-based Privileges and Access Rights, contradicting results to this survey are presented in Leander *et al.* (2019), where it is reported that role based access control is useful but not widely used. No empirical data or data collection is presented in Leander *et al.* (2019) for this statement. A plausible explanation for why role-based privileges and access rights are deemed unimportant can be found in the interviews.

The interviews covered broader cybersecurity topics and specific security controls like antivirus were not discussed. However, the topic of role-based privileges and access rights was discussed in interviews with OT personnel. An example of why this security control could be deemed as unimportant is highlighted with an anecdote of a workaround with the following quote "To be honest, it is so much easier just to use a colleague's username and password than to call the helpdesk. There are many notepads with login credentials floating around" the statement is extracted from a section of the interview when the topic revolved around communication. The helpdesk was staffed with English-speaking personnel for this specific organization, a hurdle too big for the OT personnel to overcome. If the reason for diverting the implemented security control is a lack of readily available support in your native language, a communication barrier or some other reason, for example, time pressure, as reported in Chowdhury *et al.* (2019) is not for this study to conclude. Organizations of many participants in the survey indeed have access management in place, but the workaround with "notepads with colleagues login floating around" indicates why participants do not think it is an important security control. To contextualize the sharing of login credentials "floating around" it is worth highlighting that the OT environment is prohibited and physically closed off for unauthorized personnel. Physical protection, fences and gates are ranked in the fourth place on usage and the third place on importance. The feeling of physical protection could be a mitigating factor for employees having login credentials visible in the production area even though they acknowledge that this violates organizational policies.

Specific OT cybersecurity training is the security control with the lowest usage, but it is still a security control that the survey participants recognize as important. A similar finding that lack of OT training is an area for improvement is found in Evripidou *et al.* (2023). Interestingly, training is classified in the social part of STS and even though there are few security controls in the social dimension in the survey instrument, this result could indicate that STS gaps exist. Furthermore, deeming humans the weakest link in cybersecurity (Kruger *et al.*, 2020; Kannelønning and Katsikas, 2023), it is fascinating that specific OT training receives such a low score, because knowledge, skills and understanding are the main attributes influencing cybersecurity behavior (Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015). These attributes could be improved with specific OT training.

The findings mainly focused on the challenges identified in Lars Halvdan Flå *et al.* (2024) because this reference used almost precisely the same criteria for selecting participants as we did in our work. The organizations are all within the same geographical area, making comparison accurate, because, for example, differences in culture and legislation can be excluded.

The four most compelling items are asset management, vulnerability management, IDS and patch management. All these systems are strongly or weakly linked together. They can all be used independently, but effectiveness and efficiency will improve when they interact.

Asset management is considered the most important of the four security controls, with participants placing it in sixth place. Also, asset management usage is much higher than that of other security controls, which ranked in the 10th place. However, as pointed out in Evripidou *et al.* (2023) and Lars Halvdan Flå *et al.* (2024), having an asset management system also requires asset discovery, which is a substantial challenge for OT organizations. Hardware will be replaced in an OT production facility and asset inventory updates must be made regularly. One way to have an up-to-date asset management database is by using automated systems that collect information on assets in the network. Take IDS as an example. The primary design of IDS is to detect malicious activities in the network and warn the asset owner of a possible breach. However, as pointed out in Lars Halvdan Flå *et al.* (2024), IDS can also be used to discover assets and maintain the asset management system. Knowing the installed assets is crucial for considering if vulnerabilities are present and if a patch is required. In this survey, no automated system other than IDS was introduced for the recipients, something that could create blind spots of the reality regarding the use of automated systems to maintain asset management systems. What is true is that the use of IDS is low, all the way down to 20th place and it is even lower, 23rd place for importance. One potential reason for the low score on importance could be that the participants do not know IDS. However, the degree of "I don't know" responses to IDS are in line with the other security controls, indicating that the participants do have knowledge about IDS. With no other information regarding how organizations update their asset management systems, it is impossible to conclude that the systems in use are not updated regularly. However, the IDS results indicate that regular maintenance and updates of asset management systems could be a potential improvement area.

Furthermore, why is having up-to-date asset information important? Vulnerability management, a system that checks whether your installed assets contain vulnerabilities, could work without input from an asset management system. However, the input data would be the same, some sort of supplier's component ID, and hence, it is reasonable to assume that the systems often are used in conjunction. According to the findings, this is not true, as vulnerability management is reported to almost not be used at all, 22nd place and 21st place on importance. Interestingly, the responses for vulnerability management have a high number of "I don't know" responses, almost at the threshold of being removed from the data set with 29% "I don't know" responses. One possible explanation for the low vulnerability management scores could be IT operating and maintaining vulnerability management rather than OT. If this is the case, it could explain the poor scores for such an important security control. No further investigation into how organizations manage and organize vulnerability management systems has been done in this study. What is true is that the information from vulnerability management systems is crucial for organizations for their decision to install a remedy, a patch, for known vulnerabilities.

The last security control highlighted in the findings section that deviates from best practice is patch management. Patching, either lack of or delayed patching, has been attributed as the culprit for several of the most famous cyber-attacks like NotPetya and Equifax. The consequences and benefits of patching are well documented and known for IT professionals (Souppaya *et al.*, 2018). The participants were asked: *All new patches are known and a procedure is established for OT patch management.* This question only received a score, placing the usage of patch management in the 18th place and an importance score equivalent to the 19th place. What does this finding mean? The "I don't know" option is low for this security control, indicating that patch management is a well-known security control among the participants. One reason for the lack of patching could indicate that the asset and vulnerability management results are accurate. If organizations are not the

beholders of information regarding their assets and vulnerabilities, patching a complex OT production site would be difficult, if not impossible. One thing that separates patch management from operating a vulnerability management system is that it is crucial to understand the system where a patch will be installed. So, while vulnerability management can be operated by IT, patching in the OT environment is undoubtedly a task in which OT needs to be involved. Consequently, the lack of patching is likely accurate because all respondents are from OT. However, some mitigating factors speak in favor of the lack of patching in the OT environment. There is a risk that a new patch will affect the component or system and, therefore, the system will not operate as before the patch. With OT systems highly dependent on availability and narrow time windows for maintenance (Evripidou *et al.*, 2023; Martin Gilje Jaatun *et al.*, 2021), patching might be a security control where the risk affiliated with the remedy is higher than the reward. No further investigations have been done to unearth the reason or rationale for this lack of patching in the OT environment.

Communication was the most frequent topic in the thematic analysis. IT expressed the urgency and importance of communicating risk to the business units to convey the message that cybersecurity is a business enabler. Hence, it is in everyone's interest to partake in the collective effort. OT participants expressed that the rationale for following a security control is not effectively communicated and thereby just acts as a barrier to completing one's task or work duties (Evripidou *et al.*, 2023). also highlights communication between IT and OT as one of three critical barriers for organizations to overcome in cybersecurity, the other two being governance and cybersecurity expertise (Evripidou *et al.*, 2023). points to the difference in mindset as a source for communication problems. OT, who possesses the "engineering mindset" with a strong focus on the stability and service of a system and IT, who has a "technology mindset" and is more willing to implement new technology without the same degree of mindfulness regarding the state of operations of the OT system. Such differences can lead to poor communication between IT and OT, communication that is a prerequisite to ensuring optimal cybersecurity practices (Evripidou *et al.*, 2023). No further investigation into how mindset on the individual or group level affects communication has been investigated in this study. Nor how communication is executed in the organizations, for example, type of message, communication platform used or similar. However, it is evident that IT struggles to communicate in a way that gets the organization on board to deal with cybersecurity in a joint effort. Furthermore, OT points out that security controls are barriers to completing one's task. However, there were no indications from any OT interview that they provided IT with suggestions for improvement or descriptions of pain points regarding cybersecurity, showcasing communication issues between both parties. It seems instead that OT focus their attention on finding workarounds to the perceived or actual hinderance that comes with cybersecurity instead of communicating with their IT counterpart. One of the participating CISOs highlights this: "If we do not get feedback, it is impossible to know the impact cybersecurity has on the organization."

Following communication, the topic *removal of freedom* was the second most highlighted code from the analysis. Whatever the perceived or actual removal of freedom consists of, processes, policies or technical-related issues, all participants, both IT and OT, agree that whenever a rule or a security control is perceived to be a too significant inconvenience, it will lead to workarounds. Several OT participants highlighted the path to workarounds when employees get frustrated: "We need creative problem-solving employees, which is crucial for continuous operation. However, they are also great at finding workarounds."

Two pathways are potential avenues for remedying how OT perceives this removal of freedom. First, it relates to the governance structure and how security is governed in the organization and second, it relates to communication. Governance structure: all participants

were asked how security is governed in their organization and whether today's governance structure is optimal. All agree that having too rigid and paternalistic governance would lead to unwanted situations where workarounds flourish and there will be a lack of ownership culture for security in the organization. Regarding the second part of the question, how today's governance structure is optimal, the responses differ widely. From an IT perspective, the rules are strict but fair. From the OT perspective, this is not the case. It is too hard and cumbersome to follow the organization's rules. Several point to the fact that personal responsibilities and tasks still need to be fulfilled, but in an environment that lacks the flexibility of the past. Interruption of an individual's primary tasks has been shown to have a detrimental effect on cybersecurity behavior (Chowdhury *et al.*, 2019).

The second path is communication in relation to removal of freedom. It has been highlighted earlier in this paper that IT regards communication as an essential topic. However, in the context of removal of freedom, OT participants emphasize that the users do not understand why they need to use a security control or why a process needs to be followed. The lack of explanation of why, in conjunction with miscommunication, the security team's use of terminology and language, which only a specialist can understand, is specified by participants as a problem area.

So, what might be the reasons for this situation unfolding at the participating organizations and how can some of the issues be mitigated? The failure of communication and the removal of freedom will lead to workarounds that are testaments to failed security efforts. Regarding communication, it is interesting to look at how participants perceived cybersecurity and what it consists of. In a distilled and compressed version, the OT perspective is that *cybersecurity is a technical issue outside the OT domain*. Having this view of cybersecurity is not beneficial for an organization, especially when joint cybersecurity efforts are the goal. One way to mitigate this issue is by considering how cybersecurity is governed and who is part of the governance team. By including OT in cybersecurity governance, it is reasonable to believe that the communication of why security controls are mandatory will be communicated better when OT personnel are part of delivering the message, that is, the avoidance of use of specialized terms and language. Furthermore, including OT in the governing cybersecurity team should provide more accessible feedback on pain points and the barriers to day-to-day operation. Identification of such barriers should improve the fulfillment of personal tasks. By adjusting the governance team with the inclusion of OT, it is reasonable to suggest that the number of workarounds should decrease.

Regarding the removal of freedom, statements like "things were so much easier in the past" flourished throughout the interviews. This might be true, but it is also true that security was almost nonexistent in OT in the pre-Industry 4.0 era. With the new age of interconnected OT systems, security is not voluntary but mandatory. One way to close the cultural gap of "everything was better in the past" is through improved knowledge. Knowledge has been shown by (Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015) to be one of the critical attributes for improving cybersecurity-compliant behavior, including the reduction of workarounds.

In earlier work, participants in the Norwegian Industry responded to a survey self-assessing their cybersecurity-related behavior (Kannelønning and Katsikas, 2023). This study was not limited to OT personnel but was limited to those used within an organization that operates within the Norwegian industry. The main finding showed that individuals self-identifying as having low technical knowledge were more inclined to reveal their most used password. Technical knowledge was the differentiator between those who revealed sensitive data and those who did not. This study produced favorable results, indicating that employees within the Norwegian Industry act according to their self-assessment and their organization's

policies. These favorable results were attributed to the high level of training received within the organizations. 71% of the participants had received training concerning IT security.

According to the survey data, the security control with the highest delta between usage and importance is specific OT cybersecurity training. Participants believe they do not receive the training they think is important. It is reasonable to suggest that OT personnel's knowledge levels would increase through more specific OT cybersecurity training, leading to a better understanding of *why* security controls are in place. With improved knowledge and a better understanding of *why* security controls are imposed, the perceived or actual removal of freedom leading to workarounds should decrease.

6. Conclusion

The results and discussion in this paper stem from interviews and survey results collected from the Norwegian Industry, with a focus on cybersecurity for OT systems. Several interesting findings emerge that lead to some concrete recommendations for improving the security programs of OT organizations. The way such organizations structure their cybersecurity efforts should, to a larger extent, include personnel from OT. Higher participation and collaboration between IT and OT should improve how OT personnel perceive cybersecurity, a view that today comprises cybersecurity as belonging within the domain of IT and, hence, is not an OT problem. Furthermore, by including OT in cybersecurity governance, it is believed that the identified problems regarding cybersecurity communication should be improved. Through increased training, the knowledge levels of OT staff should improve and a better understanding of why security controls are in place should lead to fewer workarounds. Increased knowledge levels are a crucial attribute for cybersecurity-compliant behavior (Hwang *et al.*, 2017; Alzahrani, 2021; Parsons *et al.*, 2015), therefore, increased specific cybersecurity training seems like an excellent organizational investment because humans are perceived in literature as the weakest link in cybersecurity. Increased training, categorized in the social dimension, would also contribute to moving the needle toward a balanced STS. A balanced STS should result in the highest value outcome for organizations (Al Sabbagh and Kowalski, 2012). Furthermore, as the OT knowledge level improves, the identified gaps between best practices and the current results regarding usage and importance of the security controls, vulnerability management and patch management should be bridged. However, it is worth noting that IT and OT systems have differences and it is therefore not to expect that future use of all security controls should be similarly deployed even though the security controls are found to be important in literature and from past cyber-attacks.

The results of this study should be of interest to practitioners in OT cybersecurity as the results provide concrete areas that practitioners can investigate in their respective organizations. The social gaps identified, including the recommendation to include OT in cybersecurity governance, should be relevant for practitioners to follow-up to reduce the number of workarounds found in this study. Furthermore, the realization that OT employees do not understand *why* security controls are in place should be of value as new OT-specific training programs are needed in organizations.

The following suggestions for future research aim to increase the study's contribution to the academic sphere and development of theory. Although socio-technical gaps have been identified, this study cannot conclude that these are the only socio-technical gaps present in OT organizations. Therefore, expanding the survey instrument to include more social elements should be developed to determine the depth of socio-technical gaps in OT organizations. Furthermore, research should also try to determine to what degree a balanced STS yields the best performance for OT organizations. Communication has frequently been

identified within the text as an area for improvement. Further research should investigate how communications are performed in organizations, how communication is framed, what media is used and whether such cybersecurity communication is done haphazardly or in a systematic order. The interplay between IT and OT with what has been identified as a lack of bi-directional communication also deserves to be investigated further.

Notes

[1.] https://ecolonical.org/quali-quanti-articles/

[2.] The NIST CSF v2.0 had not been released at the time when the survey was performed.

References

Alzahrani, L. (2021), "Factors impacting users' compliance with information security policies: an empirical study", *International Journal of Advanced Computer Science and Applications*, Vol. 12 No. 10.

Al Sabbagh, B. and Kowalski, S. (2012), "ST(CS) 2-featuring socio-technical cyber security warning systems", in *Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec)*, *IEEE*, pp. 312-316.

Bada, M., Sasse, A.M. and Nurse, J.R.C. (2019), "Cyber security awareness campaigns: Why do they fail to change behaviour?", arXiv preprint arXiv:1901.02672.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

Brooks, J., McCluskey, S., Turley, E. and King, N. (2015), "The utility of template analysis in qualitative psychology research", *Qualitative Research in Psychology*, Vol. 12 No. 2, pp. 202-222, doi: 10.1080/14780887.2014.955224.,

Bryant, A. and Charmaz, K.E. (2007), *The SAGE Handbook of Grounded Theory. Sage*.

Chowdhury, N.H., Adam, M.T.P. and Skinner, G. (2019), "The impact of time pressure on cybersecurity behaviour: a systematic literature review", *Behaviour and Information Technology*, Vol. 38 No. 12, pp. 1290-1308, doi: 10.1080/0144929X.2019.1583769.

Christine, D.I. and Thinyane, M. (2022), "Socio-technical cyber resilience: a systematic review of cyber resilience management frameworks", *Digital Transformation for Sustainability: ICT-Supported Environmental Socio-Economic Development*, Springer, pp. 573-597.

Corallo, A., Lazoi, M. and Lezzi, M. (2020), "Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts", *Computers in Industry*, Vol. 114, p. 103165.

Da Veiga, A. (2016), "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument", in *2016 SAI computing conference (SAI)*, *IEEE*, pp. 1006-1015.

Davies, R., Coole, T. and Smith, A. (2017), "Review of socio-technical considerations to ensure successful implementation of industry 4.0", *Procedia Manufacturing*, Vol. 11, pp. 1288-1295, doi: 10.1016/j.promfg.2017.07.256.,

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O. and de Blanes-Sebastián, M.G. (2025), "Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity", *Future Business Journal*, Vol. 11 No. 1, p. 28.

Djebbar, F. and Nordström, K. (2023), "A comparative analysis of industrial cybersecurity standards", *IEEE Access*, Vol. 11.

Evripidou, S., Uchenna, D., Ani, S., Hailes S. and Watson, J.D.M. (2023), "Exploring the security culture of operational technology (OT) organisations: the role of external consultancy in

overcoming organisational barriers", in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, *UCL*, pp. 113-129.

Francis, J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M.P. and Grimshaw, J.M. (2010), "What is an adequate sample size? Operationalising data saturation for theory-based interview studies", *Psychology and Health*, Vol. 25 No. 10, pp. 1229-1245.

Fred, E., Emery S. and Trist, E.L. (1960), "Socio-technical systems", *Management Science, Models and Techniques*, Vol. 2, pp. 83-97.

Giannelli, C. and Picone, M. (2022), *Editorial "Industrial IoT as IT and OT Convergence: Challenges and Opportunities*", MDPI, Vol. 3, pp. 259-261.

Hennink, M. and Kaiser, B.N. (2022), "Sample sizes for saturation in qualitative research: a systematic review of empirical tests", *Social Science and Medicine*, Vol. 292, p. 114523.

Herath, T. and Rao, H.R. (2009), "Protection motivation and deterrence: a framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 106-125.

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F. and Zhou, J. (2011), "Factors affecting perception of information security and their impacts on IT adoption and security practices", *International Journal of Human-Computer Studies*, Vol. 69 No. 12, pp. 870-883, doi: 10.1016/j.ijhcs.2011.07.007.

Hwang, I., Kim, D., Kim, T. and Kim, S. (2017), "Why not comply with information security? An empirical approach for the causes of non-compliance", *Online Information Review*, Vol. 41 No. 1.

IEC (2009), *IEC 62443-1-1 Industrial Communication networks - Network and System security - Part 1-1*, IEC, International Electrotechnical Commitee, Geneva.

Jean-Christophe, G. and Pochwatko, G. (2008), "Sometimes it is not so bad to decide in a hurry: Influence of different levels of temporal opportunity on the elaboration of purchasing intention", *Polish Psychological Bulletin*, No. 4, pp. 208-209.

Kannelønning, K. and Katsikas, S. (2023), "A systematic literature review of how cybersecurity-related behavior has been assessed", *Information and Computer Security*, Vol. 31 No. 4, pp. 463-477, doi: 10.1108/ICS-08-2022-0139.

Kannelønning, K. and Katsikas, S. (2023), "Cybersecurity-related behavior of personnel in the Norwegian industry", in *International Symposium on Human Aspects of Information Security and Assurance (HAISA)*, (Eds) Furnell, S and Clarke, N, Springer, University of Kent, Canterbury, UK, Vol. 674, pp. 249-258.

Kannelønning, K. and Katsikas, S. (2024), "Deployment of cybersecurity controls in the Norwegian industry 4.0", presented at the *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES '24), ACM, Vienna, Austria*, 07/24, 188.

Kannelønning, K. and Katsikas, S. (2024), "Usage of cybersecurity standards in operational technology systems," presented at ", *The 10th Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems (CyberICPS 2024)*, Bydgoszcz, Poland.

Khadka, K. and Ullah, A.B. (2025), "Human factors in cybersecurity: an interdisciplinary review and framework proposal", *International Journal of Information Security*, Vol. 24 No. 3, pp. 1-13.

Kruger, H., Du Toit, T., Drevin, L. and Maree, N. (2020), "Acquiring sentiment towards information security policies through affective computing", in *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Kimberley, South Africa*, 25–27 Nov. 2020 pp. 1-6, doi: 10.1109/IMITEC50163.2020.9334134.

Lars Halvdan Flå, C.A., Thieme, M., Gilje J. and Hanssen G.K. (2024), "Cybersecurity challenges in industrial control systems: an interview study with asset owners in Norway," presented at the *10th Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (CyberICPS 2024), ACM, Bydgoszcz, Poland, 09.24*.

Leander, B., Čaušević, A. and Hansson, H. (2019), "Applicability of the IEC 62443 standard in industry 4.0/IIoT", in *14th International Conference on Availability, Reliability and Security, ARES 2019, University of Kent, Canterbury, United Kingdom*, doi: 10.1145/3339252.3341481, available at: www.scopus.com/inward/record.uri?eid=2-s2.0-85071722239&doi1145%2f3339252.3341481&partnerID=40&md5=8bd37771cd2a3be336f8fbd99ddf9362

Leszczyna, R. (2018a), "A review of standards with cybersecurity requirements for smart grid", *Computers and Security*, Vol. 77, pp. 262-276.

Leszczyna, R. (2018b), "Cybersecurity and privacy in standards for smart grids – a comprehensive survey", *Computer Standards and Interfaces*, Vol. 56, pp. 62-73, doi: 10.1016/j.csi.2017.09.005.

Lezzi, M., Lazoi, M. and Corallo, A. (2018), "Cybersecurity for industry 4.0 in the current literature: a reference framework", *Computers in Industry*, Vol. 103, pp. 97-110, doi: 10.1016/j.compind.2018.09.004.

Malatji, M., von Solms, S. and Marnewick, A. (2019), "Socio-technical systems cybersecurity framework", *Information and Computer Security*, Vol. 27 No. 2, pp. 233-272, doi: 10.1108/ICS-03-2018-0031.

Martin Gilje Jaatun, E., Wille, K., Bernsmed S. and Kilskar S.S. (2021), "Grunnprinsipper for IKT-sikkerhet i industrielle IKT-systemer", in *IKT-sikkerhet – Robusthet i petroleumssektoren 2020*, *SINTEF*, available at: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2835081/ID4+apport+til+KT-sikkerhet++obusthetpdf?sequence=2

Malatji, M., Marnewick, A. and von Solms, S. (2020), "Validation of a socio-technical management process for optimising cybersecurity practices", *Computers and Security*, Vol. 95, p. 101846, doi: 10.1016/j.cose.2020.101846.

Mirtsch, M., Blind, K., Koch, C. and Dudek, G. (2021), "Information security management in ICT and non-ICT sector companies: a preventive innovation perspective", *Computers and Security*, Vol. 109, p. 102383, doi: 10.1016/j.cose.2021.102383.

Nigel King (2004), "Essential guide to qualitative methods in organizational research", London: SAGE Publications Ltd, pp. 256-270, available at: https://sk.sagepub.com/books/essential-guide-to-qualitative-methods-in-organizational-research

NIST CSF Version (2018), *Framework for Improving Critical Infrastructure Cybersecuritys*, NIST, National Institute of Standards and Technology, Gaithesburg, MD, USA.

Nüßer, W., Koch, E., Trsek, H., Schumann, R. and Mahrenholz, D. (2017), "Cyber security in production networks — an empirical study about the current status", in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), CRIS*. pp. 1-4, doi: 10.1109/ETFA.2017.8247725, available at: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=8247725&ref=

Øyvind Arntzen, T. (2022), "An effect analysis of ISO/IEC 27001 certification on technical security of Norwegian grid operators", in *2022 IEEE International Conference on Big Data (Big Data). IEEE*, pp. 2620-2629, doi: 10.1109/BigData55660.2022.10020529.

Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C. (2015), "The influence of organizational information security culture on information security decision making", *Journal of Cognitive Engineering and Decision Making*, Vol. 9 No. 2, pp. 117-129, doi: 10.1177/1555343415575152.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010), *Human Factors and Information Security: Individual, Culture and Security Environment*, Defence Science and Technology Organisation Edinburgh (Australia) Command.

Reeves, A., Parsons, K. and Calic, D. (2020), "Whose risk is it anyway: how do risk perception and organisational commitment affect employee information security awareness?", in *HCI for Cybersecurity, Privacy and Trust*, Springer International, Cham, pp. 232-249.

Robert, P., Bostrom, L., Stephen, J. and Heinen, L. (1977), "MIS problems and failures: a socio-technical perspective. Part I: the causes", *MIS Quarterly*, Vol. 1 No. 3, pp. 17-32.

Rogers, R.W. (1985), "Attitude change and information integration in fear appeals", *Psychological Reports*, Vol. 56 No. 1, pp. 179-182.

Rothenberg-Elder, K. (2023), "The qualitative methodology: Scientific justification", in *Farewell and new beginning: The Psychosocial Effects of Religiously Traditional Rites of Passage*: *Springer*, pp. 101-116.

Sony, M. and Naik, S. (2020), "Industry 4.0 integration with socio-technical systems theory: a systematic review and proposed theoretical model", *Technology in Society*, Vol. 61, p. 101248, doi: 10.1016/j.techsoc.2020.101248.

Souppaya, M., Stine, K., Simos, M., Sweeney, S. and Scarfone, K. (2018), *Critical Cybersecurity Hygiene: patching the Enterprise*, National Institute of Standards and Technology.

Stouffer, K., Pease, M., Tang, C.Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., Thompson, M., (2023), *Guide to Operational Technology (OT) Security: NIST SP 800-82, Revision 3*, National Institute of Standards and Technology, Gaithersburg, MD, USA.

Sulaiman, N.S., Fauzi, M.A., Wider, W., Rajadurai, J., Hussain, S. and Harun, S.A. (2022), "Cyber–information security compliance and violation behaviour in organisations: a systematic review", *Social Sciences*, Vol. 11 No. 9, p. 386.

Thakur, M. (2024), "Cyber security threats and countermeasures in digital age", *Journal of Applied Science and Education (JASE)*, Vol. 4 No. 1, pp. 1-20, doi: 10.54060/a2zjournals.jase.42.

Walker, G.H., Stanton, N.A., Jenkins, D., Salmon, P., Young, M. and Aujla, A. (2007), "Sociotechnical theory and NEC system design" in *Engineering Psychology and Cognitive Ergonomics: 7th International Conference, EPCE 2007, Held as Part of HCI International 2007, Beijing, China, July 22-27, 2007. Proceedings 7*, Springer, pp. 619-628.

Wagner, P., Hansch, G., Konrad, C., John, K.H., Bauer, J. and Franke, J. (2020), "Applicability of security standards for operational technology by SMEs and large enterprises", in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), CRIS*, 8–11. Vol. 1, pp. 1544-1551, doi: 10.1109/ETFA46521.2020.9212126, available at: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=9212126&ref=

Whitman, M.E. and Mattord, H.J. (2019), *Management of Information Security*, 6 ed., Cengage, pp. 220 -221.

Witte, K. (1993), "Message and conceptual confounds in fear appeals: the role of threat, fear, and efficacy", *Southern Communication Journal*, Vol. 58 No. 2, pp. 147-155, doi: 10.1080/10417949309372896.

Yin, R.K. (2018), *Case Study Research and Applications*, 6 ed., Sage, p. 319.

Corresponding author
Sokratis K. Katsikas can be contacted at: sokratis.katsikas@ntnu.no