# The role of organizational and social factors for information security in a nuclear power industry

Kristina Gyllensten
*Department of Occupational and Environmental Medicine, Sahlgrenska University Hospital, Goteborg, Sweden, and*
Marianne Torner
*School of Public Health and Community Medicine, Institute of Medicine, University of Gothenburg, Goteborg, Sweden*

Received 29 April 2021
Revised 25 August 2021
22 October 2021
29 October 2021
Accepted 2 November 2021

## Abstract

**Purpose** – The aim of this study was to explore the organizational and social prerequisites for employees' participative and rule-compliant information security behaviour in Swedish nuclear power production and its related industry. These industries are high-risk activities that must be meticulously secured. Protecting the information security in the related organizations is an essential aspect of this.

**Design/methodology/approach** – Individual in-depth interviews were conducted with 24 employees in two organizations within the nuclear power industry in Sweden.

**Findings** – We found that prerequisites for employees' participative and rule-compliant information security behaviour could be categorized into structural, social and individual aspects. Structural aspects included well-adapted rules, knowledge support and resources. Social aspects included a supportive organizational culture, collaboration and adequate resources, and individual aspects included individual responsibility.

**Originality/value** – The qualitative approach of the study provided comprehensive descriptions of the identified preconditions. The results may thus enable organizations to better promote conditions important for information security in a high-risk industry.

**Keywords** Organizational culture, Information security, Safety culture, Safety behaviour, Security behaviour

**Paper type** Research paper

## 1. Introduction

Protecting the safety of people and assets by limiting the risk of accidents is fundamental to any society. A prerequisite for this is to do what can be done to eliminate unintended events. However, such safety is equally dependent on protection from wilfully destructive acts. Not least in a highly digitalized world, access to information by unauthorized parties may put central societal functions at risk. Nuclear power energy production and its related industrial functions are high-risk activities that must be rigorously secured. An essential part of this is protecting the information security in the related organizations. High-risk industries have been defined as industries where work processes involve substantial risk for people and the environment, with vast potential for either major accidents as in nuclear power generation,

The study was financially supported by the Swedish Civil Contingencies Agency, which is hereby gratefully acknowledged.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 1, 2022
pp. 3-20
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-04-2021-0012

chemical production or aviation, or smaller scale incidents and occupational accidents as in timber harvesting or medicine (Grote, 2012). The nuclear power industry is a safety critical-industry where the operation, governance, processes and procedures aim to minimise the likelihood of accidents. This industry is experiencing new developments such as the integration of advanced technologies, which involves a focus on information security and the protection against external threats such as cyber-attacks (Hamer *et al.*, 2021). Nuclear power production plants cooperate closely with other types of industry, providing material and services, and handling nuclear wastes. The safety of nuclear power production is thus also dependent on the ability of such related industry to manage safety and security, not least the information security.

Information security is often defined by (1) confidentiality, ensuring that the information is available only to authorized individuals, units or processes; (2) integrity, protecting the accuracy and completeness of the information and (3) availability, ensuring that the information is accessible and useable on demand by authorized users. Information security is defined further by authenticity, accountability, non-repudiation and reliability (ISO/IEC, 2013). Information security challenges include external threats such as hackers, corporate espionage, infrastructure failures and internal threats such as non-compliance with the information security policy and even malicious computer abuse (Chulkov, 2017). The manner in which an organization handles information security can affect the ability to comply with legal demands, and to manage risks and competitive advantages (Dor and Elovici, 2016). Clearly, organizations need to protect their information assets from unauthorized access, and information security must include both technical and non-technical issues. Information security has been described as a multidisciplinary field that is affected by technological understanding, psychological and organizational processes and organizational structure (Wood, 2004).

Employees may contribute to a high level of information security by meticulous adherence to information security rules and procedures, that is, through compliance behaviour. A number of studies have investigated what influences individuals' motivation for information security compliance. A recent study of 2,000 Swedish workers found, that the work group's influence on individuals' intention to comply with information security policy was weak to moderate (Sommestad, 2018). Individual perceptions had a stronger influence, and it was concluded that information security perceptions in work groups are diverse, and decisions appear to be based on individual perceptions rather than group processes. Other studies have found that individual internal factors, such as self-efficacy and moral beliefs play a role in relation to information security compliance (Dang-Pham and Pittayachawan, 2015; Lankton *et al.*, 2019).

Information security may not be the primary goal for many employees. In fact, information security requirements may even hinder them from achieving organizational goals, since security procedures may conflict with other task requirements, or require additional work processes (Hwang and Cha, 2018). A systematic review of variables influencing compliance with information security policy found that over 60 variables had been studied in relation to compliance and that each factor only explained a small part of the variation in employees' behaviour (Sommestad *et al.*, 2014).

The European Union Agency for Network and Information Security (ENISA, 2018) stated that rule compliance is insufficient concerning information security, and that organizations should strive for active participation of the employees. Information security participative behaviour defines behaviour that is closely related to organizational citizenship behaviour (OCB) (Organ, 1988). OCB has been defined as "individual behaviour that is discretionary, not directly or explicitly recognized by the formal reward system and that in the aggregate promotes the effective functioning of the organization" (Organ, 1988, p. 4). Employees who are motivated for participative information security behaviour can identify needs and take own initiatives for improvement, beyond their strict work role. In-depth understanding of how the work organization and psychosocial working conditions influence the employees' ability and motivation to contribute to a high level of information security, both by compliant and participative behaviour, is thus important for informing interventions to further develop information security in organizations, and thus reduce societal risks.

Lack of adherence to information security rules and regulations may partly be due to paradoxical demands or value conflicts at work. Smith and Lewis (2011) defined paradox as "contradictory yet interrelated elements that exist simultaneously and persist over time" (p. 382). They stated that the interrelated elements of a paradox seem logical when viewed individually, but inconsistent or even absurd when juxtaposed. Tensions between demands appearing at the operator level of the organization (Tracy, 2004; Ripamonti and Scaratti, 2015) may present stressful goal conflicts for the employees (Pousette, 2001). To understand better employees lack of adherence to information security rules and regulations it is therefore important to elucidate the organizational values that conflict with information security values, and how these value conflicts influence the employees' reasoning and behaviour in relation to information security.

There has been little research attention paid to the role of organizational factors in relation to the management of information security (Al-Darwish and Choe, 2019). Khatib and Barki (2020) held forth that it is important to consider the organizational circumstances, not only individual perceptions, when trying to understand non-compliance in information technology (IT) contexts. Factors, such as organizational security culture and climate, and sanctions (Alfawaz *et al.*, 2010; Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2014), have been found to influence information security compliance. Likewise, Hooper and Blunt (2019) found that a poor organizational culture contributed to breaches in information security. Organizational information security culture has been defined as "shared patterns of thought, behaviour, and values that arise and evolve within a social group based on communicative processes influenced by internal and external requirements, are conveyed to new members, and have implications on information security" (Hallberg *et al.*, 2017, p. 22). Various factors, including management, training, awareness, policies and national culture, have been found to influence information security culture (da Veiga and Martins, 2017). There is, however, a need for deeper and more contextualized knowledge of organizational factors that influence employees' ability and motivation for compliant as well as participative behaviour to protect the information security in organizations, and not least those with critical importance to preserve societal function and safety.

The aim of this study was to inductively explore the prerequisites for information security and employees' participative and rule compliant behaviour protecting information security in nuclear power industry organizations.

This article is structured into the sections research method, findings and discussion.

## 2. Research method

This section is structured into procedure, participants and data analysis.

### *2.1 Procedure*

Quantifiable measures are often seen as the gold standard for the investigation of human aspects of information security. However, different and deeper insights can be gained by also using qualitative approaches (ENISA, 2018). Qualitative studies can provide rich perspectives and further insights into attitudes, behaviours and social processes in information security contexts. In the present study, a qualitative design was used to provide in-depth understanding of organizational and social phenomena influencing compliant and participative behaviour in relation to protecting the information security. The interview guide was developed to capture important aspects of employees' information security behaviour. In order to be open for any themes that emerged from the data, and limit the influence of preconceptions intrinsic to a predefined theoretical framework, an inductive, bottom-up approach (Braun and Carke, 2006) was applied. The questions, and what they aimed to capture, are presented in Table 1.

**Table 1.**
Interview questions

| Question<br>Please describe . . . | Phenomena that the questions aim to capture |
|---|---|
| a) a situation where you have taken own initiative to protect or improve information security at your workplace | Participative information security behavior – organizational citizenship behavior (Organ, 1997) |
| b) a situation where you have not meticulously followed the prescribed information security rules or procedures | Compliant information security behavior |
| c) a situation where it was difficult to follow the information security rules, as they conflicted with other important organizational goals | Organizational value conflicts and information management (Karlsson *et al.*, 2017) |
| d) how you would rate the general priority of information security within your workgroup, in relation to demands on efficiency and quality | Organizational culture and climate (Schneider, 1975, 1990; Schneider and Reichers, 1983; Schneider *et al.*, 2017) |

We collected the data by conducting individual in-depth interviews with 24 employees in two organizations within nuclear power production and its related industry in Sweden. The interviews were performed according to the critical incident technique (CIT) (Flanagan, 1954), which limits the influence of the interviewer's subjectivity and preunderstandings. The CIT also enables the informants to access context-specific memories and personal experiences of situations relevant to the subject matter (Druskat and Wheeler, 2003; Grill and Nielsen, 2019). The interviews took place in secluded meeting rooms at the interviewees' respective workplaces. Both authors acted as interviewers, and both have substantial previous experience in qualitative work life and safety research. Initially, four pilot interviews were conducted to assess the interview guide and assure inter-interviewer alignment in performing the interviews. The pilot interviews were recorded, transcribed verbatim and read and discussed by the authors. Both interview guide and inter-researcher alignment were found acceptable, and the four interviews were included in the analysis. Prior to and during the interviews, the participants were instructed to reflect on the four subjects presented in Table 1.

During the interviews, the participants were encouraged to describe these situations as fully and accurately as possible. The interviewers guided the participants through open follow-up questions only, and refrained from introducing any themes of their own. Each interview lasted 25–70 min. All interviews were recorded and transcribed verbatim. Ethics approval was obtained from the Swedish ethics review authority (no 2019–03386).

### *2.2 Participants*

Three Swedish worksites within two organizations in nuclear power production and its related industry took part in the study. Related industry refers to industry that is not directly involved in nuclear power production, but that is vital and closely related to the nuclear industry, by provision of material or services or storage of nuclear waste. The informants were selected through a process inspired by maximum purposeful variation sampling (see Patton, 1990), to allow a broad spectrum of personal and contextual preconditions to be explored. They were selected to increase the likelihood of acquiring rich data in terms of varied empirical accounts of experiences in relation to the research question. In total, 24 individuals participated, representing a variety of professions and work experience, see Table 2 for demographic details of the participants.

### *2.3 Data analysis*

The interviews were analysed through inductive thematic analysis (Braun and Clarke, 2006). This method was considered suitable, as it is a theoretically flexible approach that can provide a rich, detailed and complex account of the data. The analysis was conducted in accordance with Braun and Clarke (2006) and the coding was done manually using pen and markers. In the first stage, both authors read the transcripts and made analytical notes. Each transcribed interview was then coded line by line by the first author. From this initial coding, abstract themes were created. These were then refined and organised into main, overarching themes. The themes were reviewed, defined and labelled by the first author. It was important to strengthen the inter-rater reliability and therefore the results of the analysis were continuously discussed with the second author, further refined and discussed iteratively, until consensus was reached on the thematic category structure and content. In all, five such analytical meetings were held until a final list of themes was agreed upon. An example of the analytical process can be seen in Table 3.

## 3. Findings

Overall, six main themes and a number of subthemes, describing the prerequisites for information security participative and rule-compliant information security behaviour, emerged from the analysis, see Table 4. The themes, described below, could be categorized into structural, social and individual aspects. Each quote is referenced with the organization and number of the participant, for example O1P2 (organization 1, participant 2).

### *3.1 Structural aspects*

This section is divided into the following sub-sections: Well-adapted and fully accepted rules, Education and well-adapted knowledge support and Adequate resources.

| Organization, gender and age | Numbers and years |
|---|---|
| Organization 1 – nuclear power production | 12 (3 managers) |
| Organization 2 – related industry | 12 (3 managers) |
| Men | 14 men |
| Women | 10 women |
| Mean age | 49 years (SD = 9.97) |
| Departments where participants worked | HR, research, communication, security, operations, IT, finance, service and development |

**Table 2.** Demographic details of participants

| Unit of analysis | Code | Subtheme | Main theme |
|---|---|---|---|
| *"It is the knowledge in the group, I think. We have a project team . . . and it feels like the team has knowledge about this, so this becomes natural . . . One always has to find out and double-check what is ok and not ok to send. And to show. But it feels like we solve this pretty well together"* | Team has shared knowledge, support each other to know and interpret the information security rules | Support from colleagues | Supportive organizational culture and empowerment |
| *"You can't send a document with trade secrets via mail; it cannot be done"* | IT-system is helping the employees to follow the information security rules | Supportive technology, and continuous adaptation between rules and technology | Well-adapted and fully accepted rules |

**Table 3.** Example of the analytical process

| Main themes | Subthemes |
|---|---|
| *Structural aspects* | |
| Well-adapted and fully accepted rules | The number, systematization and overview of rules<br>Rule legitimacy<br>Rules well adapted to the work<br>Supportive technology, and continuous adaptation between rules and technology |
| Education and well-adapted knowledge support | Knowledge and anticipation<br>Education at all stages of work experience |
| Adequate resources | General acceptance of time requirements for information security<br>Availability of expert support<br>Dependence on external resources |
| *Social aspects* | |
| Supportive organizational culture and empowerment | High level of risk awareness and security priority<br>Supportive leadership<br>Support from colleagues<br>Support from experts |
| Collaboration and coordination | Internal collaboration and coordination<br>External collaboration |
| *Individual aspects* | |
| Individual responsibility and personality | Responsibility for the organizational goals<br>Balance between supportive systems and individual responsibility and autonomy<br>Personality |

**Table 4.**
Organizational prerequisites for participative and rule compliant information security behaviour

### *3.2 Well-adapted and fully accepted rules*

This main theme consisted of four sub-themes: The number, systematization and overview of rules; Rule legitimacy; Rules well adapted to the work and Supportive technology and continuous adaptation between rules and technology.

*3.2.1 The number, systematization and overview of rules.* The participants reported that the very large number of information security rules made it difficult to get an overview of them. The ability and experience to search for and understand information security rules differed between the employees and it could be a challenge to find the correct information.

> They can be pretty extensive, these instructions and rules . . . it is not that easy to sit down and read through one of those instructions. (O1P1)

Well-systematized rules are therefore fundamental, not least to encourage inexperienced employees to find out more about the information security rules and thus ensure compliance. The degree of detail in rules and procedures must also be well balanced and contextually adapted. Overly generic rules create uncertainty, while too much detail increases complexity.

*3.2.2 Rule legitimacy.* The information security rules were generally perceived to be helpful in guiding various aspects of the work, but information regarding why the rules and policies exist is important to create legitimacy for the rules. Fully understanding the purpose of the rules, and the threats that they are meant to control, is important for rule compliance. However, there can be a conflict between creating rule legitimacy by sharing information about a potential threat, and a security need to keep the existence of such a threat confidential. Continuous training is an important means to maintain rule legitimacy.

> There is also a dilemma with the potential threat that it too is confidential, so there is a pedagogical problem to explain to people, "Why is this important?" . . . It is difficult to motivate somebody to

> protect themselves against something that one is not allowed to speak about . . . and I think retraining is important. (O2P23)

The responsibility to gain knowledge about the security rules was largely placed on the individual employee. The application of the regulations might sometimes be difficult to interpret, and the follow-up by the management to ensure that the employees had acquired sufficient knowledge and understanding of the rules and procedures was considered insufficient.

*3.2.3 Rules well adapted to the work.* Generic information security rules worked well for most employees, while for some groups and in certain situations such generic rules were not compatible with specific work tasks. This became a problem when there was a lack of resources, ability or will to find solutions for contextual adaptation. Some rules were then viewed as impossible to follow. Other times, the rules were experienced as tedious, and shortcuts were taken to increase efficiency.

> You should not use USB memories for this. But many times there was no other possibility, and then we did it, anyway, which meant breaking the rules. (O2P22)

Since the information security rules highly impact employees' ability to perform their work efficiently and well, employees often approach the security departments with needs for better adaptation. This engagement was experienced by the recipients as inspiring, but also as adding to their workload.

*3.2.4 Supportive technology, and continuous adaptation between rules and technology.* An IT system with build-in checkpoints, supporting and guiding compliance with information security rules, was viewed as helpful, particularly in relation to tasks that were performed seldom. It eliminated certain mistakes and shortcuts.

> You can't send a document with trade secrets via mail; it cannot be done. (O2P21)

Although participants shared relevant examples of how IT systems provided support, there was a wish for further support from the IT systems.

> Well, what you have to do when you introduce this kind of rule, I think, is to thoroughly think it through . . . "What about the support in the IT system? Can the people working with this do their jobs without becoming totally frustrated?" Because if you do not, people will find the shortcuts really quickly. (O2P24)

Participants emphasised the importance of the IT systems being user friendly to avoid frustration and shortcuts.

*3.2.5 Education and well-adapted knowledge support.* This main theme consisted of two sub-themes: Knowledge and anticipation and Education at all stages of work experience.

3.2.5.1 Knowledge and anticipation. At an initial stage of a task or project, the knowledge to choose an adequate level of security of documents was sometimes insufficient. This, in combination with the fact that the procedure of changing the security level at a later stage was cumbersome, encouraged "over-safing". A high security level was then set "just in case", sometimes unnecessarily restricting the possibility to share the document. This caused inefficiency and frustration.

3.2.5.2 Education at all stages of work experience. The need for education and training, in order to learn and remember information security rules, was highlighted by many participants. In this type of industry, the employees must be knowledgeable in a wide range of safety-related areas. However, especially for the newly employed, no matter how good the education programmes are, this presents a dilemma. A new employee faces learning constraints due both to the time required to take the courses to acquire sufficient information in all these areas and to the cognitive load it implies to integrate all this information into knowledge. The importance of adequate time and quality of the introduction training, with good mentorship, was emphasized, as well as a need to pilot test all new courses, in order to evaluate and optimize them before full-scale implementation. To keep the issue of information security in the fore, and to be relevant and effective, education should be continuous and closely coupled to concrete work tasks. Education was not only viewed as a matter for new hires; continuous education was also considered important for employees who had been working at the organization for a long time.

> Maybe we care about teaching the newly hired, but all these "old foxes" who have been here for many, many years, they probably work like they always have done, and I think it is easy to forget them. (O2P16)

Certain aspects of information security can be very complex and require a lot of time and training to learn. Education could help to increase awareness of the rules and to raise the topic for discussion.

*3.2.6 Adequate resources.* This main theme consisted of three sub-themes: General acceptance of time requirements for information security; Availability of expert support and Dependence on external resources.

3.2.6.1 General acceptance of time requirements for information security. Following the information security rules was often more time consuming than breaking them and taking shortcuts, but many expressed that there was a general acceptance of these time requirements.

> One takes information security for granted . . .. It is a prerequisite for doing the job, so you can never say, "I do not care about it." Rather, information security is a rule that we have to follow. And under the condition that one follows that rule, one works as effectively as possible. In the daily business in my department we do not talk that much about information security, we talk a lot about efficiency. But this is always with the understanding that information security rules are followed. (O1P5)

Information security was afforded the time needed to implement it. According to some participants, there were no repercussions when projects took longer than planned due to information security requirements.

3.2.6.2 Availability of expert support. It was important that the department responsible for information security had enough time and resources to deal with questions and issues that emerged in the operating departments. When this was not the case, the security departments became bottlenecks.

> Then there is a problem that the IT-expert has a lot to do, which means that he cannot always prioritize giving us the decision we need to get on with our work. So, I can see that there is a problem, that he has a heavy workload which means that delays occur. If it is really important stuff, critical stuff, yes of course, then there is no doubt. (O1P9)

When problematic issues were not dealt with in a timely way, this caused frustration at the operational level.

3.2.6.3 Dependence on external resources. The resources of external parties had an influence on the ability to work in accordance with information security rules. An example of constraints related to external resources was encryption systems in other organizations, such as authorities, that were not compatible to the ones used in the nuclear industry. Another example that was held forth was the external security examination of new members of staff.

> One example of this, if you work in a high security organization, is background checks where the security police are involved. And when that rule was introduced, the waiting time was two weeks. Now suddenly there is a waiting time of six to eight weeks. This means an extreme amount of hassle and extremely high costs. The more of those issues, the higher the drive to ignore the rules. If the

> rules are perceived to be bureaucratic, difficult to follow, ineffective and so on, then one tends not to follow them. (O1P14)

Examples were given of delays in security examination having taken such a long time that highly qualified job applicants had chosen other work.

### *3.3 Social aspects*

This focuses on the social aspects and is divided into the following sub-sections: Supportive organizational culture and empowerment and Collaboration and coordination.

*3.3.1 Supportive organizational culture, and empowerment.* This main theme consisted of four sub-themes: High level of risk awareness and security priority; Supportive leadership; Support from colleagues and Support from experts.

3.3.1.1 High level of risk awareness and security priority. Questions relating to information security were much present in daily work, and many described a high awareness of these issues in the organizations.

> It feels like it is in the culture somehow . . . to have this at the back of one's mind. "Is this ok to show someone else?" And it feels like we think like that all the time, or at least, I do. And I think that most of the people at my department would reply something similar as well. (O1P12)

Some participants described that this awareness was embedded in the organizational culture.

3.3.1.2 Supportive leadership. The managers at all levels were viewed as strong role models in the work with information security, and it was important that they should lead by example. This was also consistently considered to be the case. According to some informants, the CEO signalled the importance of highlighting mistakes or work practices that could lead to breaches in security, including information security. The senior management were considered sincere and credible in their claims for security priority. They signalled that information security is important, both by leading training on the topic and by backing up employees persevering in adherence to security procedures in situations where information security had become an issue of conflict in relation to corporate or external parties.

> Our senior management is really trying to spread this message, that these types of issues are important. We have a basic security training course that everyone should complete . . .. And they have now revised the structure of the course, updated it for all employees, and someone in the senior management team has led it each time. (O1P3)

> We have a clearly pronounced mentality in this company, I would say, that security comes first, and that is the case for all situations, regardless of whether it relates to personal safety, information security or something else. All employees have the right to say, "Stop, this is not ok", without being considered the black sheep. And it is very clearly communicated all the way from the CEO that he expects this, too. (O1P9)

The management provided positive feedback to employees who stood up for the information security and listened with interest to employees' suggestions for further security development. If needed, the managers also took over the practical dealing of errands that had induced conflict between employees and superiors in external parties.

3.3.1.3 Support from colleagues. Support from colleagues was a salient issue in most of the interviews. It played an important role in the awareness, mutual understanding and interpretation of the information security rules.

> It is the knowledge in the group, I think. We have a project team . . . and it feels like the team has knowledge about this, so this becomes natural . . . One always has to find out and double-check what is ok and not ok to send. And to show. But it feels like we solve this pretty well together. (O1P12)

Discussions between colleagues, on different aspects of information security and on how rules should be interpreted, are an important way to learn and to raise awareness and there was a wish for more opportunities for such discussions. Groups of colleagues spontaneously gathered in order to try to solve a problem together, or to develop a common interpretation of complex rules. Sometimes the rules were not clear-cut and the discussions with colleagues helped to find common strategies in dealing with these situations. The colleagues also provided support in balancing different important values such as information security and efficiency. Recurrent peer dialogues and discussions created normative consensus on how rules should be interpreted and implemented, and reduced the risk of individuals drifting and deviating in security behaviour. Dialogues regarding information security increased reflection and made the topic more connected to everyday practice.

An open and no-blame culture was described, where it was acceptable to make errors and this seldom resulted in sanctions, but where it was socially unacceptable to try to cover-up such errors. It was also considered socially acceptable to point out others' errors, as long as this was done respectfully and constructively. Several participants expressed that even the socially demanding actions of correcting persons in higher positions in the organizational hierarchy were accepted.

> [Informant's reaction to having been corrected by a colleague]: What did I say? Well, I thanked him, like, "Ha, ha!" And I said "Well done," because it was a pretty new guy that said it, so it was right. (O2P23)

Newcomers are mentored and actively socialized into a culture of personal responsibility. This creates not only group cohesion and role clarity but also peer control, since deviant behaviour spills over negatively, affecting how the entire team is perceived.

3.3.1.4 Support from experts. Information security experts provided support to employees, and participants reported that these experts generally had a welcoming and open attitude that encouraged employees to approach them with questions. It was important to be able to get in contact with the experts easily and quickly. However, work overload at the security departments could delay responses to issues that did not have the highest priority (see sub-section Availability of expert support). Also, employees who perceived their ability to work as very restricted by the information security regulations, requested substantially more dialogue and engagement from the security experts, to find solutions that would be acceptable for both parties.

*3.3.2 Collaboration and coordination.* This main theme consisted of two sub-themes: Internal collaboration and coordination; and External collaboration.

3.3.2.1 Internal collaboration and coordination. Collaboration between different internal departments and teams was important in order to share and develop ways to work in accordance with information security rules. An organization of task-based areas of responsibility created role clarity and also distinct role limits. Different functional units had their own organizational logics. This contributed to "downpipes" and counteracted coordination between different parts of the organization. There was a degree of an "us and them" mentality between different geographical establishments of the organizations. Many meetings could be handled via electronic media, but sometimes meetings needed to be in person to overcome these obstacles.

> The challenge is to communicate so that we understand each other. It can be both them and us . . . but we still have to try to get them to understand. But we should also try to understand them . . .. And then, if you are in the same place, it works . . . and then it seems like we understand each other. (O2P18)

More and better communication between the IT security and the specialist departments was requested, in order to find solutions that were acceptable for both parties. It was highlighted that the IT systems were designed to fit the standard user, which worked well in most cases. But it was also important to spend more time and resources to find solutions for the more specialized users, to enable them to work effectively. The need for better knowledge among the experts about the time requirements for project administrators' information security tasks was also underscored. This would enable better coordination, and thus, better quality of work, and reduce time pressures and stress in both functions.

3.3.2.2 External collaboration. When collaborating with external parties, the information security rules can create disturbances and make the process tortuous.

> And we said, "No, but these are classified documents, so you cannot have them. In that case they have to be sent by paper." They wanted us to scan and mail them. "No, we cannot do that." They talked to the CEO because they were so upset that we followed . . .. Of course, we cannot say that we will make an exception [laughs] to our information security rules. So, there are different cultures. (O2P16)

The use of commonplace software, which supported task performance but did not hold sufficient security, was restricted. This presented controversy between parties and reduced the efficiency of collaboration. It was foreseen that increased digitalization might increase conflicts in the collaboration with both corporate and external parties, as well as the number of security threats. The sharing of paper documents is easier to control than that of electronic ones. Also, the use of electronic conference media limits the possibility to know and control who is participating in a meeting.

The communication with public authorities could sometimes be problematic. One example was when different laws contradicted each other, one requiring openness and another confidentiality. Swedish law prescribes a high degree of public access to information in public authorities. It was therefore considered a risk that secret documents sent to public authorities might unintentionally become public. Established international cooperation on nuclear security issues, with information security being one, was stressed as important and beneficial.

### *3.4 Individual aspects*

This section is focused on the main theme Individual responsibility and personality.

*3.4.1 Individual responsibility and personality.* This main theme consisted of three sub-themes: Responsibility for the organizational goals; Balance between supportive systems and individual responsibility and autonomy and Personality.

3.4.1.1 Responsibility for the organizational goals. Many expressed a strong individual responsibility for working in accordance with the information security rules and for taking action to develop information security. Taking individual responsibility for security was considered an important part of the work for all.

> Individual responsibility is an important part of maintaining the security. So, it is about taking a lot of initiatives, so I try to take a lead in that way. (O1P7)

3.4.1.2 Balance between supportive systems and individual responsibility and autonomy. It was considered important to have a balance between necessitating systems support and detail in rules and procedures, on one hand, and individual vigilance and responsibility, on the other. Critical reflection, challenging current practice and being open to further development were mentioned as important. It was highlighted that there is a risk with a system that is overly controlling or specified. Such a system may deprive the individual of the sense of personal responsibility, and thus counteract vigilance, critical reflection and the incentive to act in a participative manner.

> One can build that ideal system where all documents, all mails, everything should be, but then you alienate the human being; in other words, he or she feels that they lack control – I'm monitored and can stop thinking about security. (O2P21)

However, while a certain degree of autonomy and room for interpretation was considered important, it was emphasized as essential to make conservative judgements "when in doubt".

3.4.1.3 Personality. Individual differences and personality influence whether the employee takes responsibility to follow and develop the ongoing work of information security. Some participants clearly stated that risk-takers, or persons with little patience with sometimes cumbersome procedures, are not well-suited to work in this type of industry.

> Yes, people differ, we are different . . . what should I say, in how willing we are to take risks. It is not that great if there are too many risk-takers in the nuclear business [laughs]. (O1P1)

In summary, the themes that emerged from the analysis were categorized into structural, social and individual aspects of employees' information security behaviour. In the following section relevant previous research and practical implications will be outlined.

## 4. Discussion

The current study explored the prerequisites for employees' participative and rule-compliant behaviour for protecting information security in organizations in nuclear power production and its related industry. Six main themes emerged from the interviews and these were categorized into structural, social and individual aspects. Below, the results will be discussed in accordance with these aspects. The main themes were: Well-adapted and fully accepted rules; Education and well-adapted knowledge support; Adequate resources; Supportive organizational culture and empowerment; Collaboration and coordination and Individual responsibility and personality.

### *4.1 Structural aspects*

The structural aspects consisted of three main themes: Well-adapted and fully accepted rules, Education and well-adapted knowledge support and Adequate resources. In the following sub-sections, each of the themes will be discussed in relation to previous literature.

*4.1.1 Well-adapted and fully accepted rules.* The first theme, *Well-adapted and fully accepted rules*, highlights that well-systematized, legitimate information security rules, well adapted to the work to be performed, are important to ensure compliance. The degree of detail in the rules must be well balanced and contextually adapted. Too much detail increases complexity, while overly generic rules create uncertainty. Grote (2009) suggested that security sometimes could be enhanced by flexible rules that can be adapted according to the situation, and argued that there needs to be a good balance between flexible and stable rules that are adapted to the specific organization. Our results are also in concordance with those presented by ENISA (2018), in a review of the information security literature. It was there concluded that non-secure behaviour is mainly driven by security being too effortful and/or too complex, and it was argued that information security practices need to accept that human attention and effort is a precious resource predominantly devoted to productivity. Hence, information security should fit into work processes, instead of disrupting them.

*4.1.2 Education and well-adapted knowledge support. Education and well-adapted knowledge support* was the second main theme found in the study. Information security rules can be very complex and require a lot of time to learn, and it was highlighted that continuous, adequate training to learn and remember information security rules was important. The interviews pinpointed an important dilemma. In high-risk industry, a newly employed needs immediate knowledge on a range of security and safety issues. At this stage of the career, one is particularly reliant on formal rules and procedures, since one has little or no experience to guide one's actions securely in different situations. However, there is, for one, a limit to how much time can be spent on education and training, and also perform the core tasks. In addition, learning a new job is a comprehensive cognitive task, and therefore the ability to take in and process information regarding a wide range of safety related issues at this stage, when it is needed the most, is much limited. This highlights the importance of further pedagogics development and complementary forms of learning in this type of industry. Previous research has found that training, together with factors such as management, awareness, policies and national culture, also influences the information security culture (da Veiga and Martins, 2017).

*4.1.3 Adequate resources.* The main theme *Adequate resources* highlighted the acceptance of the extra time often required for working in accordance with information security procedures. Such procedures may involve additional workload and having to deal with complex technology, which can lead to increased levels of work stress (Hwang and Cha, 2018). Information security may not be the primary goal for many employees and can conflict with core task requirements. Previous studies have found that many employees fear the consequences of not being sufficiently productive more than the consequences of being responsible for a cybersecurity incident (Kirlappos *et al.*, 2015; Beautement *et al.*, 2016; ENISA, 2018). Under certain circumstances, information security may be violated when the benefit of compliance is lower than the cost of compliance (Bulgurcu *et al.*, 2010; Hwang and Cha, 2018). Clearly, it is essential that managers are accepting of the fact that following information security rules may involve additional time.

The lack of external parties' resources sometimes caused delays, and examples were given of delays in security examination of job applicants having taken such a long time that highly qualified applicants had chosen other work. This induces a threat to ensuring company competence.

### *4.2 Social aspects*

The social aspects consisted of two main themes: Supportive organizational culture and empowerment; and Collaboration and coordination. In the following sub-sections, each of the themes will be discussed in relation to previous literature.

*4.2.1 Supportive organizational culture, and empowerment.* A poor organizational culture has been found to contribute to breaches in information security (Hooper and Blunt, 2019). This points to social phenomena, captured in the fourth theme identified in the present study, *Supportive organizational culture and empowerment*. This theme highlights the importance of supportive leadership, and support from colleagues and security experts. In safety culture and climate research, the importance of managers' unrebutted priority of safety is well-established (Christian *et al.*, 2009; Beus *et al.*, 2010). Organizational cultures, and thus safety and security cultures, also comprise social norms among co-workers, and Jackson (2017) found that co-worker social support and trust was important for individuals to internalize group safety priorities and validate the individual's sense of competency. This sense of competency was important in dealing with work ambiguity. Similarly, it has been suggested that individuals turn to each other for social verification when cues are ambiguous (Festinger, 1954; Weick, 1995). A study on organizational practices and information security found that improving information security performance required innovative practices to encourage knowledge sharing among employees (Perez-Gonzalez *et al.*, 2019).

In the present study, the informants emphasized the importance of frequent and spontaneous discussions between colleagues, on different aspects of information security and on how rules should be interpreted and situationally implemented. This was a way to learn and raise awareness, but not least, to develop a common interpretation of rules and find common strategies to apply them in ambiguous work situations. It has been suggested that cybersecurity needs acts of "heroism" in dealing with novel threats, and these acts can only be performed by employees who are skilled, engaged, trusted and supported by the organization (Pfleeger *et al.*, 2014). In the current study, participants expressed that support and feedback from colleagues and management increased empowerment and motivation to take initiatives to improve information security. A work climate where it is socially acceptable to, respectfully and constructively, question or criticize the behaviour of colleagues and superiors was put forth as important. Such behaviour requires a high level of mutual trust and empowerment.

*4.2.2 Collaboration and coordination.* The main theme *Collaboration and coordination* referred to the role of internal and external collaboration in relation to information security. In the current study, the organizational logic sometimes differed between units or specialized departments within the organization. When this difference was large, which was sometimes the case, it created mistrust and substantial problems in the coordination between different parts of the organization. Previous studies have reported problems with the collaboration between security specialists and employees, with one-way communication from the security specialists, and employees avoiding seeking advice, which led to problems difficult to fix and disagreements over security controls (Ashenden and Sasse, 2013). In concordance, ENISA (2018) pointed out the need to improve the collaboration between security practitioners and other organizational functions.

### *4.3 Individual aspects*

The final main theme, *Individual responsibility and personality*, highlighted the role of the individual employee in information security practice. The literature emphasizes that organizations need employees who are empowered and can act to deal with rapidly emerging information security threats (Kirlappos *et al.*, 2015). In the current study, participants clearly expressed that they took personal responsibility for developing information security and saw themselves as important agents to protect the security of the organization. Furthermore, the participants expressed the importance of balancing individual responsibility and necessitating systems support. An overly controlling system can deprive the employee of a sense of responsibility. Grote (2015) found that safety, in certain situations, can be improved with flexible rules that can be adapted according to the specific circumstances and argued that it is important that individuals are encouraged to think freely and speak up if they observe problems. Overconfidence in safety systems may lead to complacency, which is often held forth as an underlying cause of major accidents (Årstad and Aven, 2017).

The role of personality in information security awareness has been studied, and factors such as agreeableness, emotional stability, conscientiousness and propensity for risk-taking have been found to play a role (McCormac *et al.*, 2017). However, ENISA (2018) concluded that personality is seldom linked to security behaviour in a consistent way. In the current study, the participants pointed out that “a risk-taking personality” did not belong in the nuclear industry. Some participants also pointed out that since a high-risk industry will always be highly regulated, with a large number of rules and procedures, it requires employees with patience enough to endure and uphold such a cumbersome work style.

### *4.4 Implications*

The nuclear power industry is generally known for a high level of awareness of potential hazards (Hamer *et al.*, 2021). The two organizations participating in the present study also displayed a high level of information security awareness and practice. The results highlight organizational and social aspects that are important prerequisites for information security and can therefore guide further safety and security development in different types of high-risk industry. High-risk industry, being in the forefront in terms of information security management, also offers learning opportunities regarding factors of high importance for information security for other types of industry, where safety and security are not issues equally embedded in the organizational culture.

Based on the findings the following recommendations can be made:

*4.4.1 Structural aspects.*

(1) Develop well-adapted information security rules with a balance between flexibility and stability and facilitate a continuous review of the existing rules.

(2) Ensure education and training that supports learning throughout the career, through a variety of well-adapted and tested pedagogics methodologies.

(3) Provide sufficient resources for the information security support departments, so that issues and questions can be dealt with promptly and efficiently.

(4) Accept and normalize that complying to information security rules may take additional time.

*4.4.2 Social aspects.*

(1) Foster an open and trustful organizational climate, where discussions between colleagues on the topic of information security are encouraged, and where it is socially acceptable to question constructively the behaviours of both colleagues and superiors.

(2) Have an ongoing discussion regarding information security between the information security experts, management and the different types of users, and allocate the time required to find solutions acceptable to all different parties. Encourage and allow time for frequent peer discussions on the interpretation and implementation of rules.

*4.4.3 Individual aspects.*

(1) Recognize and emphasize that information security always requires individual responsibility, and that each employee thus is an essential contributor.

### *4.5 Conclusions*

Prerequisites for employees' participative and rule compliant behaviour, protecting information security in organizations in nuclear power production and its related industry, were categorized into structural, social and individual aspects. Structural aspects included well-adapted rules, knowledge support and adequate resources. Social aspects included a supportive organizational culture and collaboration, and individual aspects included individual responsibility. These factors are important to consider, to promote and facilitate information security in high-risk industry.

In terms of limitations the correctness and depth of a study of sensitive matters like security attitudes and behaviour in high-risk organizations is threatened if the participants find it difficult to be open in the interviews, not least to protect information security. In the present study, these issues were thoroughly talked through by interviewer and informant before the start of the actual interview, including voluntary participation. The interviewers informed the participants about the study, making clear that it did not aim either to disclose protected information or to find scapegoats, but rather to identify organizational phenomena that could enlighten organizational conditions that support or hamper information security practice, and that full confidentiality was ensured.

The study was confined to two organizations within nuclear power production and its related industry in Sweden, which may limit the transferability of the results. However, the sample of 24 informants was ample and employees from many different departments and with different job roles, tenure and gender contributed to descriptions of a variety of situations and aspects influencing participative and rule-compliant information security behaviour. For qualitative studies, it is also important to relate the findings to previous research and thereby add to the accumulation of results (Willig, 2013). In the current study, many of the main themes resonated with literature and theories based on previous research. While recognizing that a qualitative study cannot be generalized in the same manner as a large quantitative study, the qualitative methodology provides opportunity for a more in-depth understanding of the phenomena influencing compliant and participative behaviour in relation to protecting information security. The critical incident methodology also limits the influence of the interviewers' precognitions. The results of the study were fed back to information security experts at the participating organizations, and the results made sense to them, which strengthens the validity of the results.

## References

Al-Darwish, A.I. and Choe, P. (2019), "A framework of information security integrated with human factors", in Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, HCII 2019. Lecture Notes in Computer Science, Springer, Cham, Vol. 11594.

Alfawaz, S., Nelson, K. and Mohannak, K. (2010), "Information security culture: a behaviour compliance conceptual framework", *Paper Presented at the 8th Australasian Information Security Conference*, Brisbane, Australia, 2010, pp. 47-55.

Årstad, I. and Aven, T. (2017), "Managing major accident risk: concerns about complacency and complexity in practice", *Safety Science*, Vol. 91, pp. 114-121.

Ashenden, D. and Sasse, M.A. (2013), "CISOs and organisational culture: their own worst enemy?", *Computers and Security*, Vol. 39, pp. 396-405.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, M.A. (2016), "Productive security: a scalable methodology for analysing employee security behaviours", *Proceedings of the SPOUPS*, USENIX Association.

Beus, J., Payne, S., Bergman, M. and Arthur, W. (2010), "Safety climate and injuries: an examination of theoretical and empirical relationships", *Journal of Applied Psychology*, Vol. 95, pp. 713-727.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3, pp. 77-101.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34, pp. 523-548.

Christian, M.J., Bradley, J., Wallace, J. and Burke, M. (2009), "Workplace safety: a meta-analysis of the roles of person and situational factors", *Journal of Applied Psychology*, Vol. 95, pp. 1103-1127.

Chulkov, D.V. (2017), "Escalation of commitment and information security: theories and implications", *Information and Computer Security*, Vol. 25, pp. 580-592.

da Veiga, A. and Martins, N. (2017), "Defining and identifying dominant information security cultures and subcultures", *Computers and Security*, Vol. 70, pp. 72-94.

Dang-Pham, D. and Pittayachawan, S. (2015), "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach", *Computers and Security*, Vol. 48, pp. 281-297.

Dor, D. and Elovici, Y. (2016), "A model of the information security investment decision-making process", *Computers and Security*, Vol. 63, pp. 1-13.

Druskat, U.V. and Wheeler, J.V. (2003), "Managing from the boundary: the effective leadership of self-managing work teams", *Academy of Management Journal*, Vol. 46, pp. 435-457.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31, pp. 285-318.

ENISA (European Union Agency for Network and Information Security) (2018), "Cybersecurity culture guidelines: behavioural aspects of cybersecurity", available at: www.ensisa.europa.eu.

Festinger, L. (1954), "A theory of social comparison processes", *Human Relations*, Vol. 7, pp. 117-140.

Flanagan, J.C. (1954), "The critical incident technique", *Psychological Bulletin*, Vol. 51, pp. 327-358.

Grill, M. and Nielsen, K. (2019), "Promoting and impeding safety: a qualitative study into direct and indirect safety leadership practices of construction site managers", *Safety Science*, Vol. 114, pp. 148-159.

Grote, G. (2009), "Coordination in high-risk organizations: the need for flexible routines", *Cognition, Technology and Work*, Vol. 11, pp. 17-27.

Grote, G. (2012), "Safety management in different high-risk domains – all the same?", *Safety Science*, Vol. 50, pp. 1983-1992.

Grote, G. (2015), "Promoting safety by increasing uncertainty: implications for risk management", *Safety Science*, Vol. 71, pp. 71-79.

Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B. and Törner, M. (Eds) (2017), *Informationssäkerhet Och Organisationskultur [Information Security and Organizational Culture]*, Studentlitteratur, Lund.

Hamer, R., Waterson, P. and Jun, T. (2021), "Human factors and nuclear safety since 1970 – a critical review of the past, present and future", *Safety Science*, Vol. 133, 105021.

Hooper, V. and Blunt, C. (2019), "Factors influencing the information security behaviour of IT employees", *Behaviour and Information Technology*, Vol. 39, pp. 862-874.

Hwang, I. and Cha, O. (2018), "Examining technostress creators and role stress as potential threats to employees' information security compliance", *Computers in Human Behaviour*, Vol. 81, pp. 282-293.

ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) (2013), *Information Technology Security Techniques Code of Practice for Information Security Management*, Geneva, available at: http://docplayer.net/668061-Information-technology-security-techniques-code-of-practicefor-information-security-controls.html (accessed 10 May 2018).

Jackson, J. (2017), *Coworker Influence upon Individual Internalization of Safety*, Doctoral dissertation, Carleton University, Ottawa.

Karlsson, F., Karlsson, M. and Åström, J. (2017), "Measuring employees' compliance – the importance of value pluralism", *Information and Computer Security*, Vol. 25, pp. 279-299.

Khatib, R. and Barki, H. (2020), "An activity theory approach to information security non-compliance", *Information and Computer Security*, Vol. 28, pp. 485-501.

Kirlappos, I., Parkin, S. and Sasse, M.A. (2015), "'Shadow security' as a tool for the learning organization", *Computers and Society*, Vol. 45, pp. 29-37.

Lankton, N., Stivason, C. and Gurung, A. (2019), "Information protection behaviours: morality and organizational criticality", *Information and Computer Security*, Vol. 27, pp. 468-488.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Malcolm Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behaviour*, Vol. 69, pp. 151-156.

Organ, D. (1988), *Organizational Citizenship Behavior: the Good Soldier Syndrome*, Lexington Books, Lexington.

Organ, W.D. (1997), "Organizational citizenship behavior: it's construct clean-up time", *Human Performance*, Vol. 10, pp. 85-97.

Patton, M.Q. (1990), *Qualitative Evaluation and Research Methods*, Sage, Thousand Oaks, CA.

Pérez-González, D., Preciado, S.T. and Solana-Gonzalez, P. (2019), "Organizational practices as antecedents of the information security management performance: an empirical investigation", *Information Technology and People*, Vol. 32, pp. 1262-1275.

Pfleeger, S.L., Sasse, M.A. and Furnham, A. (2014), "From weakest link to security hero: transforming staff security behaviour", *Journal of Homeland Security and Emergency Management*, Vol. 11, pp. 489-510.

Pousette, A. (2001), *Feedback and Stress in Human Service organisationsDep of Psychology*, University of Gothenburg, Gothenburg, Doctoral Thesis.

Ripamonti, S.C. and Scaratti, G. (2015), "Safety learning, organizational contradictions and the dynamics of safety practice", *Journal of Workplace Learning*, Vol. 27, pp. 530-560.

Schneider, B. (1975), "Organizational climates: an essay", *Personnel Psychology*, Vol. 28, pp. 447-479.

Schneider, B. (1990), *Organizational Climate and Culture*, Jossey-Bass Publishers, San Francisco.

Schneider, B., Gonzales-Roma, V., Ostroff, C. and West, M. (2017), "Organizational climate and culture: reflections on the history of the construct in JAP", *Journal of Applied Psychology*, Vol. 102, pp. 468-482, January (Online First Publication).

Schneider, B. and Reichers, A.E. (1983), "On the etiology of climates", *Personnel Psychology*, Vol. 36, pp. 19-39.

Smith, W. and Lewis, M. (2011), "Toward a theory of paradox: a dynamic equilibrioum model of organizing", *Academy of Management Review*, Vol. 36, pp. 381-403.

Sommestad, T. (2018), "Work-related groups and information security policy compliance", *Information and Computer Security*, Vol. 26, pp. 533-550.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22, pp. 42-75.

Tracy, S.J. (2004), "Dialectic, contradiction, or double bind? Analyzing and theorizing employee reactions to organizational tension", *Journal of Applied Communication Research*, Vol. 32, pp. 119-146.

Weick, K. (1995), *Sensemaking in Organizations*, Sage, Thousand Oaks, CA.

Willig, C. (2013), *Introducing Qualitative Research in Psychology*, McGraw-Hill Education, London.

Wood, C. (2004), "Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature", *Computer Fraud and Security*, Vol. 1, pp. 16-17.

**Corresponding author**
Kristina Gyllensten can be contacted at: kristina.gyllensten@vgregion.se