REDISET

Resilient Digital Sustainable Energy Transition

Manual for conducting reality checks on human cyber security vulnerabilities in the Nordic electricity based digitalized energy system

LINDA TURTOLA | PETRA BERG | MANSI NEGI | BAHAA ELTAHAWY | MAZAHER KARIMI | KARINA BARNHOLT-KLEPPER | SONJA MONICA BERLJIN

UNIVERSITY OF VAASA REPORTS 54

University of Vaasa

VAASAN YLIOPISTO

Publisher University of Vaasa
School of Marketing and Communication, Marketing.

Authors Linda Turtola
Petra Berg https://orcid.org/0000-0002-7899-3458
Mansi Negi https://orcid.org/0000-0003-2560-7282
Bahaa Eltahawy https://orcid.org/0000-0001-6372-7547
Mazaher Karimi https://orcid.org/0000-0003-2145-4936
Karina Barnholt-Klepper
Sonja Monica Berljin https://orcid.org/0000-0002-3809-3156

Project report
ISBN 978-952-395-195-2 (pdf)
URN http://urn.fi/URN:ISBN:978-952-395-195-2

ISSN 2489-2580 (University of Vaasa Reports 54, online)

Title of publication
Manual for conducting reality checks on human cyber security vulnerabilities in the Nordic electricity based digitalized energy system

Keywords EBDES, electrification, digitalization, resiliency, cyber security

Project website
https://www.kth.se/rediset

Funder Business Finland
NordGrid Energy Research
Swedish Energy Agency

Tiivistelmä

Energian sektorin lisääntyvä digitalisaatio on tuonut mukanaan sekä mahdollisuuksia että kyberturvallisuushaasteita. Modernit sähköpohjaiset digitalisoidut energiajärjestelmät (EBDES) integroivat tekoälyä (AI), esineiden internetiä (IoT) ja älykkäitä sähköverkkoja, mikä lisää haavoittuvuuksia sosio-kyber-fyysisissä järjestelmissä (SCPS). Näiden riskien tunnustamiseksi kansainväliset instituutiot, kuten Kansainvälinen energiajärjestö (IEA) ja Euroopan unioni (EU), ovat ottaneet käyttöön sääntelykehyksiä, mukaan lukien kriittisten toimijoiden sietokykyä koskeva direktiivi (CER) ja uudistettu verkko- ja tietoturvadirektiivi (NIS2), vahvistaakseen kyberturvallisuutta.

REDISET-hanke (2022–2025) vastaa tarpeeseen kehittää strukturoituja lähestymistapoja sosio-kyber-fyysisten riskien hallintaan Pohjoismaiden energiasektorilla. Keskeinen lopputulos on kyberturvallisuuskäsikirja poliittisille päättäjille, turvallisuusviranomaisille ja liiketoiminnan kehittäjille, tarjoten ohjeistusta riskienhallintaan ja parhaisiin käytäntöihin. Käsikirja kokoaa hajanaista kyberturvallisuustietoa yhteen helposti lähestyttäväksi kokonaisuudeksi, jota täydentää sosiaalisen manipuloinnin tarkistuslista, jolla arvioidaan kyberturvallisuustietoisuutta ja -osaamista kyselyiden avulla. Tämä työkalu auttaa käyttäjiä arvioimaan omaa kyberturvallisuustasoaan ja priorisoimaan käsikirjan olennaisia osia.

Yksi suurimmista kyberturvallisuuden haasteista on organisaatioiden kyberturvallisuuskulttuurin, taitotason ja koulutuksen vaihtelu, mikä johtaa epäjohdonmukaisiin turvallisuuskäytäntöihin. Liiallinen riippuvuus sääntelystä ja monimutkaisten turvaprotokollien vastustus altistaa kriittiset järjestelmät uhille. Näiden ongelmien ratkaiseminen edellyttää kyberturvallisuuskoulutusta, eri sektoreiden välistä yhteistyötä ja strategisia investointeja turvallisuusinfrastruktuuriin.

REDISET-käsikirja ja tarkistuslista tarjoavat strukturoituja ja käyttäjäystävällisiä resursseja kyberturvallisuuden vahvistamiseen energiasektorilla. Edistämällä koulutusta, sääntöjen noudattamista ja sosio-teknistä riskienhallintaa käsikirja pyrkii luomaan turvallisemman ja kestävämmän energiajärjestelmän sekä varmistamaan valmiuden kehittyviin kyberuhkiin.

Abstract

The increasing digitalisation of the energy sector has introduced both operational opportunities and cybersecurity challenges. Modern electricity-based digitalized energy systems (EBDES) integrate artificial intelligence (AI), the Internet of Things (IoT), and smart grids, increasing vulnerabilities within socio-cyber-physical systems (SCPS). Recognizing these risks, institutions such as the International Energy Agency (IEA) and the European Union (EU) have implemented regulatory frameworks, including the Directive on the Resilience of Critical Entities (CER) and the Revised Network and Information Security Directive (NIS2), to strengthen cybersecurity resilience of the energy sector.

The REDISET project (2022–2025) addresses the need for structured approaches to managing socio-cyber-physical risks in the Nordic energy sector. A key outcome is a cybersecurity manual for policymakers, security officers, and business developers, providing guidance on risk mitigation and best practices. The manual consolidates fragmented cybersecurity information into an accessible resource, complemented by a social manipulation checklist that assesses cybersecurity awareness and knowledge through structured questionnaires. This tool enables users to evaluate their cybersecurity proficiency and prioritize relevant sections of the manual.

A major challenge in cybersecurity resilience is the variation in organizational cybersecurity culture, skill levels, and training, leading to inconsistent security practices. Over-reliance on regulations and resistance to complex security protocols further expose critical systems to threats. Addressing these issues requires cybersecurity education, cross-sector collaboration, and strategic investment in security infrastructure.

The REDISET manual and checklist offer structured, user-friendly resources to enhance cybersecurity resilience in the energy sector. By promoting education, regulatory compliance, and socio-technical risk mitigation, the manual aims to foster a secure and sustainable energy landscape while ensuring preparedness for evolving cyber threats.

Contents

Figures

Tables

Abbreviations

EBDES	Electricity Based Digitalized Energy System
IT	Information Technology
OT	Operational Technology
NIS2	The Revised Network and Information Security Directive
CRA	Cyber Resilience Act
CER	The Critical Entities Resilience Directive
TSO	Transmission System Operator
DSO	Distribution System Operator
ISO	International Organization for Standardization
NIST	The National Institute of Standards and Technology
IEC	International Electrotechnical Commission
AI	Artificial Intelligence
IoT	Internet Of Things
SCPS	Socio-Cyber-Physical Systems

1 INTRODUCTION

The importance of strengthening cybersecurity in the energy sector has been widely acknowledged by both academics (see for example Smith, 2021) and institutions like International Energy Agency (IEA, 2020) as well as the European Union (EU, 2024a) that has introduced new cybersecurity management legislation in recent years. In the EU, new legislative requirements, such as the Directive on the Resilience of Critical Entities (Directive (EU) 2022/2557; CER) and the Revised Network and Information Security Directive (Directive (EU) 2022/2555; NIS2), have presented new cybersecurity requirements for energy business entities recognized as operators of critical infrastructure.

The growing interdependency of societal operators, including those in the energy sector, means that a cybersecurity incident affecting one entity can lead to cascading effects across multiple systems (EU, 2024a). According to the union this leads to an expanding amount of different threat scenarios. The procedures and elements involved in energy generation, distribution, storage as well as usage are all part of the energy system in utilities, that aim to reduce environmental impact while maintaining reliable and effective energy delivery. To optimize energy production, distribution, and consumption in a sustainable manner, modern electricity-based digitalized energy systems (EBDES) utilize advanced technologies like artificial intelligence (AI), the Internet of Things (IoT), and smart grids. (Smith, 2021; IEA, 2020; EU, 2024a; Gungor et al., 2010).

Smart grids are fundamental for EBDES and are developed to provide two-way communication between energy producers and consumers by using data driven analytics. Gungor et al. (2010) describes smart grids as improved electrical networks that respond adaptively to variations in energy supply and demand by using real time data from sensors and meters. The use of smart meters and advanced metering infrastructure (AMI) that gather real time data and allow utilities to implement demand response and dynamic pricing (Fang et al., 2012). These literature studies exhibit the role of smart grid in flexible and decentralized energy systems that reflects on modern energy systems. Integration of renewable energy is integral to sustainable networks which is an aspect of digital energy systems. A lot of research bodies explore the generation from renewables such as solar and wind power in digital energy systems. Employing technologies such as predictive analytics in digital systems can estimate generation from renewable energy (Hatziargyriou et al., 2006). Technology such as artificial intelligence (AI) is crucial in enabling seamless integration by anticipating variations and controlling energy storage to address intrinsic intermittency of renewable energy (Morstyn et al., 2018). The shortfall in between the demand for renewable energy and its supply is adhered by energy storage facility, in the form of amongst others batteries. Technologies such as battery

energy storage can improve grid stability by storing excess renewable energy and releasing it when the demand is high. Effective storage management helps to maintain grid resilience and maximizes the use of renewable resources (Parra et al., 2017). Research pinpoints the importance of security measures including encrypted communication and AI based anomaly detection to protect the smart grid. Additionally, achieving seamless communication and coordination across multiple platforms is made more challenging by the incompatibility of heterogeneous devices and technologies within digitalized systems (Govindarasu, 2011). Also, Zhang et al. (2018) highlights the lack of standards in networked grids causes system integration to be more challenging and leads to inefficiency.

Digitalized energy systems also enable increased consumer engagement in the consumption and production of energy as well as active retail market participation. Mobile applications and web platforms that collect data from smart meters (Ehsan and Yang, 2018) promote digital infrastructures such as energy platforms that support the organization virtual energy collectives (Boekelo and Kloppenburg 2023) or energy communities (Envall et al., 2023), as well as individual prosumers (Campos and Marín-González, 2020). Real time data access and smart meters are considered vital elements of consumer empowerment because they allow them to study their energy usage and make knowledgeable decisions. Consumers have a chance to save energy and money by changing their energy behavior when they have access to real time consumption data through smart meters (Darby, 2010). Digitalized energy systems promote culture of sustainable energy consumption and greater transparency, which benefits the consumer and wider grid, but at the same time it introduces new security and data protection risks as it changes markets, businesses and jobs (Strielkowski et al., 2022).

Thus, the EBDES has resulted in increasingly interconnected socio-cyber-physical systems (SCPS), representing a new layer of technological interaction where physical infrastructures, such as energy systems, are enhanced with digital technologies enabling dynamic and real-time interactions between users and technologies. This allows for more decentralized and flexible systems by integrating digital technologies into the energy grid, making it more responsive to changing demands and environmental conditions as well as fosters greater user engagement (Milevskyi et al., 2023). Still, in these evolving SCPS' cybercriminals might take advantage of various types of social- physical - cyber-vulnerabilities, potentially disrupting energy systems and with serious implications on economy and society. This manual aims to highlight vulnerabilities stemming from the human – socio - interaction with the cyber-physical layers in the EBDES. It also gives suggestions to how to reduce these possible threats by describing different actor segments and their specific needs more explicitly.

1.1 The need for manual and social manipulation checklist as project drivers

The REDISET project (2022 – 2025) addresses the need for a structured approach for managing socio-cyber-physical risks in the Nordic energy sector. The main task of the fourth project work package (WP 4) was to develop a comprehensive manual for policymakers, security officers, business developers, and other key stakeholders, to help them create more understanding about socio-cultural aspects affecting cyber security in the Nordic EBDES. This manual builds upon a systematic examination of threat scenarios developed during earlier work packages (WP 2 descriptions of the future energy system in the Nordic region and WP 3 Social, physical and cyber threat scenarios) that helped capture the complexities of socio-cyber-physical systems undergoing digital transformation.

As project findings, we have discovered that there is a need for a "hands-on" manual to understand the roles and needs of different actors in the EBDES. Especially, as one of the key challenges identified was the fragmented nature of available cybersecurity information, which is dispersed across multiple sources. Thus, there is a need for a concise, user-friendly manual that presents cybersecurity guidelines in an accessible and engaging format. Moreover, the checklist and manual could serve as tools to ensure compliance and operational efficiency in complex, safety-required systems. As strict national and international regulatory frameworks, such as the EU Clean Energy Package, govern the energy sector, checklists might help implement these tasks with reduced chances of errors and ensure adherence to regulations (de Haan et al., 2021). Manuals, on the other hand, act as resources with safety procedures for handling disruptions like equipment failure or cybersecurity breaches (Smith et al., 2020). In situations like blackouts, these procedures assist in quick decision-making. They can also serve as a resource for new employees to understand processes methodologically (Hale et al., 2020). As energy systems evolve with new developments, renewable and new demand integration, and updated regulations, organizations can document changes and updates in the manual and use it as a unified resource (Zugno et al., 2022). This manual and checklist have been created to give the reader an easy systemic overview of the current challenges and possible solutions related to cyber security of the Nordic EBDES.

Recognizing the diverse roles and perspectives of stakeholders within the energy sector is crucial, as each group faces distinct challenges in navigating socio-cyber-physical complexities. Here, a marketing segmentation approach was used to specify the key stakeholder groups and main factors driving their actions in the EBDES. By examining the responsibilities and challenges of these stakeholder segments—whether end users, Transmission System Operator (TSO) personnel, or policymakers—readers gain a more comprehensive understanding of the sector's intricacies. This broader perspective fosters

a more integrated approach to problem-solving and risk mitigation within the energy domain.

To enhance engagement and facilitate self-assessment, the manual begins with the possibility to fill in the cybersecurity awareness and knowledge questionnaires. This assessment tool enables readers to evaluate their current knowledge and preparedness regarding cybersecurity threats within the digital energy ecosystem. By completing the questionnaire, users can identify specific areas of concern in the manual and thus prioritize aspects requiring further attention. Table 1. demonstrates the different levels of expertise used to measure the level of awareness and knowledge of the person.

Table 1. Levels of expertise.

Level (0-5)	Description
0 Nothing	No knowledge, completely passive.
1 Basic	Limited understanding and minimal protections.
2 Compliance-Focused	Doing enough to meet rules and regulations.
3 Proactive	Actively managing risks and improving security.
4 Integrated	Security is a key part of daily operations.
5 Leader	Leading the way and setting standards in security.

The above table 1. indicates the levels of awareness and knowledge of cyber security in the field of energy. The questionnaire is divided into two main parts, the first testing the awareness (Appendix 1. Questionnaire I AWARENESS) and the second testing the knowledge of the respondent (Appendix 3. Questionnaire II KNOWLEDGE). This means, that the respondent completing the entire questionnaire receives two scores, the first indicating the level of awareness and second the level of knowledge. Also, questionnaire II on knowledge is divided into two different "knowledge fields", where the first one measures general cybersecurity knowledge and the second is energy sector specific.

Altogether, the aim of the check list is to indicate which factors are the strongest or weakest of the one taking the test. By completing the questionnaires and looking at the scores, the checklist also provides an indication on where to look for information first in the manual. After the completing the questionnaires, the respondent can check the scores from the Appendix 2. Answers and recommendations to questionnaire I and Appendix 4. Answers and recommendations to questionnaire II. The Appendix 2 AND 4 showcases the

right answers as well as what the questionnaire respondent could especially focus on regarding cybersecurity and which parts of the manual address these challenges.

Appendix 1. Questionnaire I AWARENESS

Appendix 2. Answers and recommendations to questionnaire I

Appendix 3. Questionnaire II KNOWLEDGE

Appendix 4. Answers and recommendations to questionnaire II

Following the questionnaire, the manual provides an in-depth analysis of key actors' segments within the energy sector and their primary challenges. By exploring the specific issues faced by different stakeholder groups, readers can develop a more nuanced understanding of the interconnected challenges within the sector. This foundational knowledge helps contextualize the socio-cyber-physical risks explored in the latter sections of the manual. The manual systematically categorizes these challenges into distinct domains, including cybersecurity cultural challenges, behavioral challenges, technical challenges, and economic challenges. By structuring its analysis in this manner, the manual offers a strategic approach to risk mitigation, ultimately strengthening cybersecurity resilience within the energy sector.

2 KEY SEGMENTS OF ACTORS IN THE ELECTRICITY BASED DIGITALIZED ENERGY SYSTEM

Because of the systemic nature of the cyber challenges in the energy sector, there is a need to understand its different actors and their specific needs and challenges regarding security. REDISET project has published a system model (Berg et al., 2024), that depicts and describes 7 domains that need to stay in balance to keep the energy system functioning (see Figure 1.).

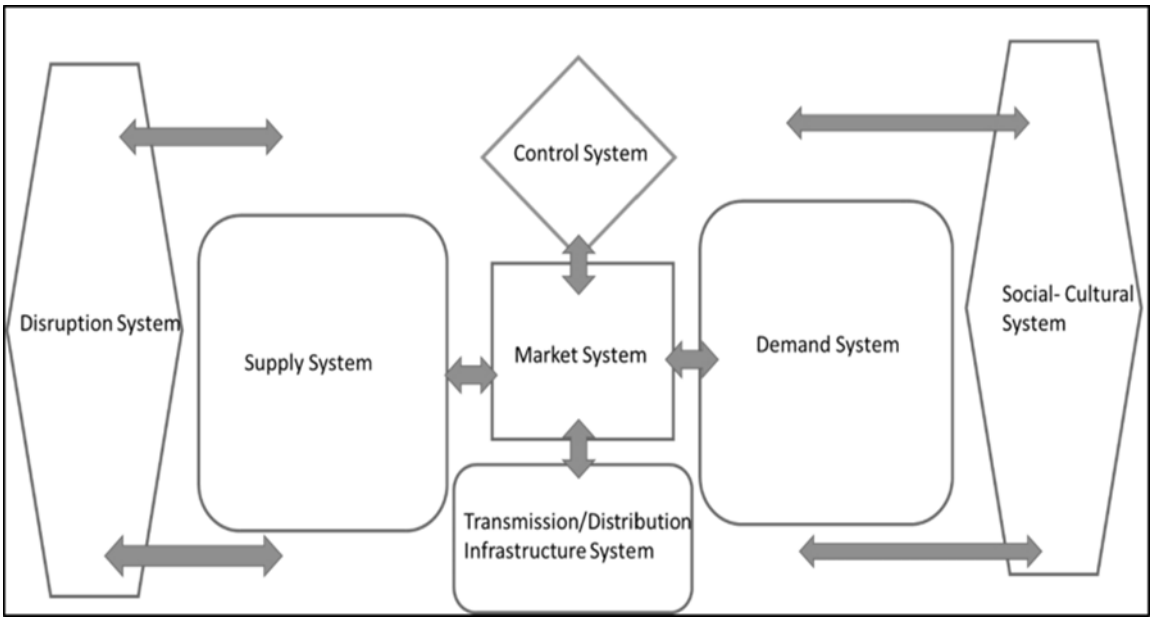

Figure 1. Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid. (Berg et al., 2024).

Based on literature reviews and project workshop results, a system-of-systems energy model that explicitly emphasizes social-cultural aspects and disruptions, was proposed. The model, as shown in Fig. 1, encompasses seven system domains, as follows: 1) supply system; 2) demand system; 3) transmission/distribution infrastructure system; 4) market system; 5) control system; 6) disruption system; 7) and the social-cultural system. As the name indicates, every system of the proposed model encompasses its own sub-systems, which might vary depending on many factors (see Berg et al., 2024).

For the system to function properly, different actors are needed to maintain it, and that is why during the research of work package 4, marketing segmentation tools were used to define and explain the key characteristics of different actors' segments. The six segments identified as key actors of the electricity-based digitalized energy system include end users, prosumers, employees in electricity-related companies, personnel working for electricity transmission and distribution operators, the defense sector, and policymakers

and market regulators. These groups were identified through stakeholder discussions, research workshops and academic literature. For the final workshop with industry representatives that was held in Vaasa, Finland in September 2024, five of these segments were chosen, with the end user segment being excluded. The reason for not including the end user segment in the final workshop and the manual was that it is a large and heterogeneous field of multiple segments who mostly do not actively participate in shaping the cyber security processes in the energy sector. Also, many central practices of end users can be related to the prosumer segment. The work with the segmentation aimed to better understand the specific factors relevant to possible cyber security challenges of each group. This chapter synthesizes workshop findings and academic literature to paint a full picture of the five segments and their perceived challenges within the cybersecurity of the energy system. The understanding of the needs of these various actors depicted in Figure 2. that participate in and maintain the EBDES has guided the choices of information included into this manual.

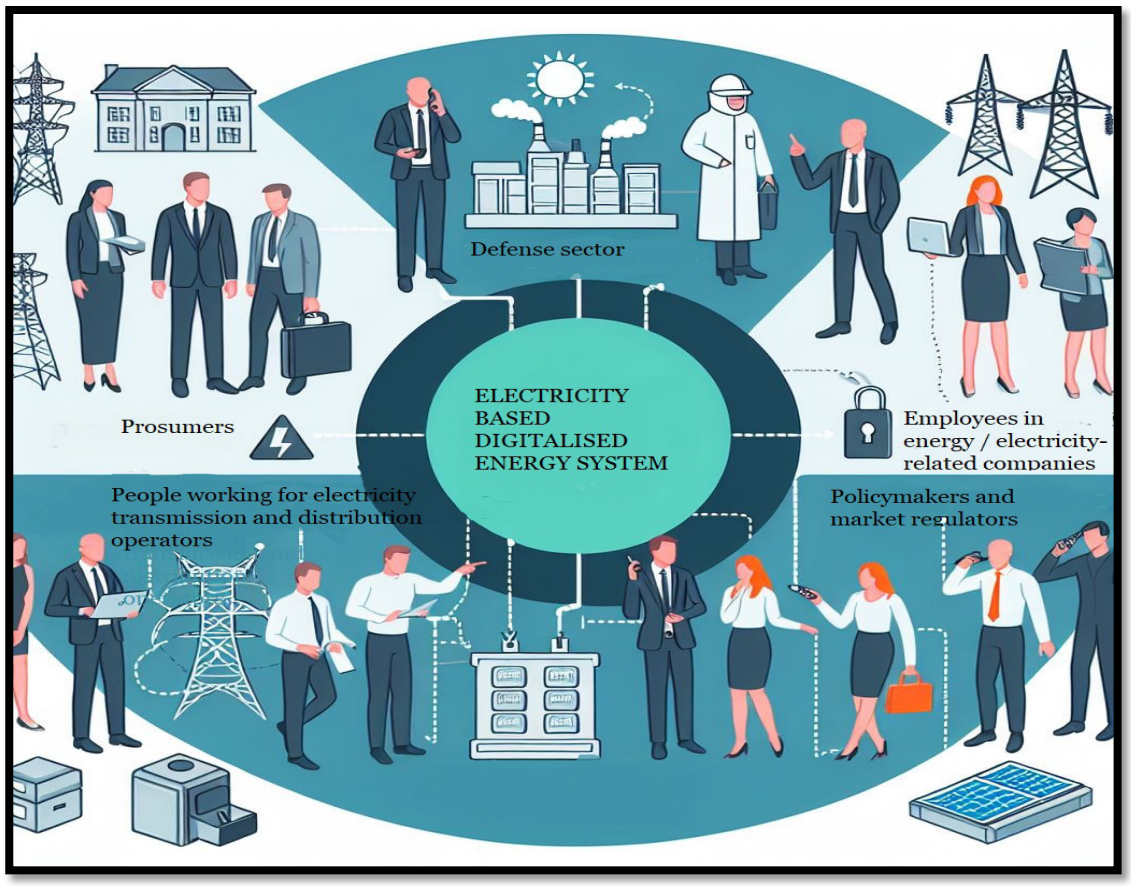

Figure 2. The different actor segments of the EBDES (made with Co-pilot 31.1.2025)

To enhance our understanding of the various actors within the energy system, we employed basic market segmentation tools. The tools, mainly consisting of a user profiling

canvas and problem tree approach, enabled us to identify and define the key segment types within EBDES and their perceived challenges. The segmentation approach involved developing a set of leading questions to create the actors' profiles. These questions were first refined to align with the project's objectives and adapted based on the differences between the segments. The segmentation canvas and its leading questions (see Fig. 3), as well as the problem tree (see Fig. 4 p. 26) were also tested through interviews with project stakeholders to ensure their relevance and accuracy.

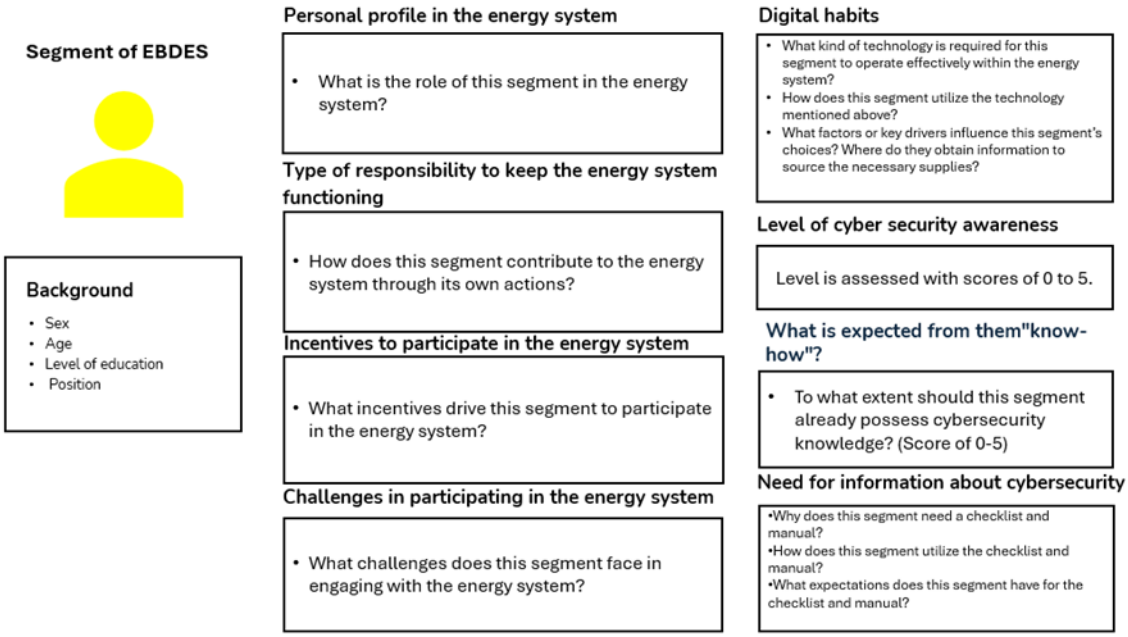

Figure 3. Segmentation tool used to categorize actors in the EBDES.

The figure (Fig. 3) above presents a structured framework for segmenting different actors and their roles within the EBDES by using key questions and headers to define each segment's responsibilities, challenges, and requirements. They are formatted to align with the system model thinking of the REDISET project's seven domains (see Fig. 1 p.6, Berg et al., 2024). The first leading question;" personal profile in the energy system" addresses the fundamental question: What is the role of this segment in the energy system? And this is further specified in the next question; "type of responsibility to keep the energy system functioning". Following that, the third question examines how each segment actively contributes by asking: How does this segment contribute to the energy system through its own actions? Then," incentives and challenges", explores participation drivers with the question: "What incentives drive this segment to participate in the energy system?" and identifies potential obstacles through "What challenges does this segment face in engaging with the energy system?". These insights help us understand what motivates or hinders different groups (social actors) in their interaction with the cyber-physical system. These aspects are explored further in the following chapter, where the section

"Drivers and Barriers in Participating in the Energy System" which is repeated for each segment, addresses the different roles, responsibilities, incentives, and challenges.

On the right side of the segmentation framework, the "digital habits" question focuses on technological engagement, posing critical questions such as: "What kind of technology is required for this segment to operate effectively within the energy system?" and "how does this segment utilize the technology mentioned above?". Additionally, it examines decision-making influences by asking: What factors or key drivers influence this segment's choices? Where do they obtain information to source the necessary supplies? In the "level of cybersecurity awareness" section, security competence is assessed using a rating from 0 to 5, answering: What is expected from them in terms of know-how? and "to what extent should this segment already possess cybersecurity knowledge?" (Score of 0-5). This helps determine their preparedness and potential need for further cybersecurity training. The findings are presented in the descriptions of each segment headlined as "Digital Habits and Anticipated Cybersecurity Awareness and Knowledge Levels". It also explores the interaction with technology and cybersecurity awareness in relation to REDISET metrics.

Finally, the "need for information about cybersecurity" section emphasizes the importance of structured guidance, addressing questions such as: "Why does this segment need a checklist and manual?" and "how does this segment utilize the checklist and manual?". It also considers expectations by asking: What expectations does this segment have for the checklist and manual? This part was not utilized directly for the segmentation but was used as a guideline for formatting the manual.

2.1 Prosumer segment

About a decade ago, following the more widespread introduction of grid connected residential photovoltaic (PV) systems and smart grids in the Nordics, prosumers began to appear in the energy sector (Kotilainen, 2020). Our findings during the REDISET project show that the definition of a prosumer is often simplified as "a producer and a consumer." This definition is also supported by academic literature, as for instance Ertz et al., (2024) propose that prosumer can be broadly defined as a person who serves as both as a producer and a consumer. Additionally, Cortade and Poudou (2022) have defined prosumer as an active consumer, who both consumes and produces electricity based on distributed renewable energy sources. Energy prosumers can be seen as "provider consumers" according to for instance Kotilainen (2019). The definition implies that energy prosumers may not in fact produce energy but provide access to their energy-related resources, such as hot water tanks or the heating system, for flexibility and demand response purposes. Especially for the energy sector, prosumers are classified as

commercial, residential, and industrial entities. (Kotilainen, 2020; Ertz et al., 2024; Kotilainen et al., 2019)

2.1.1 Drivers and barriers in participating in the energy system

The prosumer segment carries a distinct responsibility in maintaining the stability and functionality of the energy system, as it simultaneously operates as both a producer and a consumer of energy. However, various factors must be considered regarding how prosumer activities may influence the broader energy sector. According to Child et al. (2020) there are several ways that prosumers can impact the energy system. The authors point out that due to increasing levels of self-consumption, less energy may be required from centralised grids annually. The same authors do note, however, that if prosumer supply is low during times of high overall demand, transmission levels as measured by power transfer may not alter. For transmission and distribution companies, whose expenses are primarily determined by peak power loads but who have traditionally profited from moving energy to end users, this has important implications. Child et al. (2020) continue the argumentation by stating that this is a highly relevant issue in the Nordics since PV consumers will have high levels of supply in the summer, when demands are typically low, and little to no supply during the winter, when demands are typically high. Seasonal energy storage is one way to offset this temporal imbalance, but prosumers can only store energy in temporary solutions like batteries. Prosumers may ultimately affect energy markets, which could become unstable if the right precautions are not taken to prevent such problems. (Child et al., 2020).

Research conducted within the REDISET project has identified key responsibilities of prosumers in maintaining the functionality of the energy system. Chief among these is their role in distributed energy production, where they independently generate electricity for the shared energy network. While product installation must comply with established regulations, this task is typically handled by third-party suppliers, such as certified electricians. Additionally, products intended for prosumer use should carry the CE marking, indicating compliance with stringent safety, health, and environmental protection standards within the European Economic Area. However, concerns have been raised regarding the reliability of CE markings, questioning whether buyers can truly trust their authenticity. Another significant finding is the lack of sufficient monitoring of prosumers. Specifically, the absence of comprehensive legislation to regulate and restrict prosumer activities has been highlighted as a potential risk, raising concerns about challenges within the energy sector.

Prosumers have various incentives to participate in the energy system. During the REDISET project, both environmental values and the potential for cost savings—particularly by avoiding electricity distribution fees—were identified as key motivations

for prosumers engaging in the electricity market. Additionally, the REDISET project's research findings recognized other significant drivers of energy prosumerism, including the aspiration for self-sufficiency and off-grid living, as well as the opportunity to generate revenue through energy production. According to Cortade and Poudou (2022), the primary motivation for prosumers to participate in the energy system is financial savings. Beyond economic considerations, Salami et al. (2024) emphasize that sustainability concerns also play a crucial role, particularly for environmentally conscious "green consumers" who actively participate in the energy transition. Kotilainen et al. (2016) have identified multiple motivational factors influencing energy prosumerism, arguing that both internal and external drivers encourage consumers to become active prosumers. At the macro level, incentives and sanctions serve as key policy measures shaping prosumer behavior. However, Kotilainen et al. (2016) caution that such external interventions may lead to over-justification, potentially diminishing intrinsic motivation for prosumerism. Furthermore, they highlight a distinction between early and late market adopters. Early market prosumers are more likely to be intrinsically motivated and engage in activities such as co-creation, testing, validation, and providing feedback. In contrast, later market entrants tend to be driven more by extrinsic incentives. As a result, macro-level policy instruments play a critical role in fostering mass-market adoption. Kotilainen et al. (2016) assert that during the early phases of market adoption, intrinsic motivation is more influential, whereas in later phases, extrinsic factors become the predominant drivers of prosumer participation.

While prosumers have strong incentives to participate in the energy market, they also encounter significant challenges in engaging with the energy system. According to Salami et al. (2024), key barriers to prosumerism include financial constraints, limited access to information, and the absence of supportive policies, such as net metering. Discussions during the project highlighted financial challenges as a major obstacle, particularly the high upfront costs of energy equipment for individual consumers and the relatively low return on investment. The lack of supportive policies was also recognized as a critical barrier, with taxation emerging as a particularly notable concern. Furthermore, Nordic weather conditions were identified as a significant constraint, further complicating the feasibility of prosumer participation in the energy system.

2.1.2 Digital habits and anticipated cyber security awareness and knowledge levels

The REDISET project findings indicate that digital habits and technological usage within the prosumer segment play a crucial role in the adoption and diffusion of energy-related innovations. Environmental technologies often require a top-down approach, driven by policy, legislation, and regulatory frameworks. Kotilainen et al. (2016) argue that in the diffusion of innovation, there is a critical threshold at which an innovation achieves mass

adoption and becomes self-sustaining. Different types of prosumers interact with technology in distinct ways. Early adopters are typically more technologically inclined, willing to experiment with new solutions, and engage in innovation. In contrast, late adopters tend to be more risk-averse, prioritizing usability and cost-effectiveness in their decision-making (Kotilainen et al., 2016). Additionally, late adopters are generally more price-sensitive, further influencing their adoption of energy technologies.

The findings also highlight that prosumers require essential technological components such as smart meters, inverters, converters, and battery storage systems to effectively participate in the energy market. These technologies are primarily used for household applications, including charging electric vehicles. The main sources of information on technology suppliers and service providers include local electricity companies, social media, advertisements, and word-of-mouth recommendations. Beyond technical aspects, the project underscores that cybersecurity awareness among prosumers remains low, typically categorized at Level 0 or Level 1. It has been observed that "prosumer cyber awareness typically ranges from no knowledge and complete passivity to a limited understanding with minimal protections, as prosumers are generally everyday individuals without extensive cybersecurity expertise." Despite this limited awareness, compliance with existing regulations is generally considered sufficient to maintain an adequate level of cybersecurity at the prosumer level.

2.2 People working in public and private energy related organizations including both cyber and non-cyber experts

Although the working roles within public and private energy-related organizations vary across both cyber and non-cyber domains, energy infrastructure remains critical to societal and economic stability. Consequently, professionals in these organizations play a vital role in maintaining functionality, security, and efficiency. The energy sector operates as an interconnected value chain, where each stage, from resource extraction to energy distribution, contributes to sustainability, security, and stability (Carvalho, 2017; Luiijf & Klaver, 2015). Cybersecurity professionals manage digital systems such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, while engineers, technicians, and operators oversee physical infrastructure, energy production, and transmission (Fischer, 2021; Ridley, 2018). With increasing digitalization, cybersecurity and physical operations are becoming more interconnected, as security breaches in digital control systems can directly impact physical infrastructure, leading to blackouts, equipment failures, and safety risks (Salmon, 2019). The cyber-physical nature of energy production and distribution necessitates expertise across disciplines to enhance resilience against both cyber and physical threats. Findings from

the REDISET project emphasize key priorities for energy organizations, including data privacy, continuous skill development, and compliance with industry regulations. Protecting customer data, staying informed about emerging trends, and actively participating in training and legislative updates were identified as essential practices. Additionally, strict adherence to confidentiality agreements, such as NDAs and DPAs, along with the ability to deliver critical services and products, is crucial for ensuring the functionality, security, and efficiency of energy systems. Key responsibilities for maintaining the energy system include safeguarding data privacy, protecting network cables in remote locations, ensuring service continuity for a defined period, monitoring contractual compliance, upholding legal cybersecurity policies, and conducting background research for new contracts.

Data privacy is a critical concern in the digitalized energy sector, where smart grids, demand-response management, and renewable energy integration depend on vast amounts of consumer data (Gellings, 2020). The collection and processing of such data pose privacy risks, as smart meters can reveal personal consumption patterns and occupancy behaviors (Efthymiou & Kalogridis, 2010). Regulatory frameworks such as the GDPR in the European Union and the CCPA in the United States establish guidelines for data protection, transparency, and consent-based data collection (Voigt & Von dem Bussche, 2017). The evolving nature of the energy sector requires professionals to continuously update their knowledge on technological advancements, regulatory changes, and sustainability goals. Active engagement with industry trends, specialized training, and legislative developments fosters innovation and competitiveness (IEA, 2021; Georgidau et al., 2023). Case studies such as Shell's training program and Schneider Electric's Digital Academy highlight the effectiveness of structured learning programs in skill development (Shell Sustainability Report, 2020; Schneider Electric, 2021). Pursuing industry-recognized certifications further enhances employability and expertise in specialized domains (IEA, 2021).

Cybersecurity agreements such as Non-Disclosure Agreements (NDAs) and Data Protection Agreements (DPAs) play a crucial role in safeguarding sensitive information in energy organizations. The increasing sophistication of cyber threats, including phishing and ransomware, necessitates robust data protection strategies to ensure the confidentiality, integrity, and availability of critical systems (Alcaraz & Lopez, 2014). Ensuring the continuous operation of energy systems also requires technical expertise, a commitment to sustainability, and a customer-centric approach. The integration of digital tools such as artificial intelligence (AI), machine learning, and the Internet of Things (IoT) enhances predictive maintenance, energy optimization, and consumer engagement, ultimately improving system efficiency and resilience (Mylrea & Gourisetti, 2017).

2.2.1 Drivers and barriers in participating in the energy system

The REDISET project has identified several key incentives that encourage professionals in both public and private energy-related organizations, including cyber and non-cyber experts, to actively engage in the energy system. These incentives include the ability to optimize work-related energy usage, enhance company competitiveness, and foster greater proactivity in the energy market. Additionally, professionals are motivated by the opportunity to improve system optimization, ensure the proper functionality of energy infrastructure, and maintain the sustainability and safety of materials through cost and quality assessments. Financial incentives also play a significant role in encouraging active participation. The global transition in the energy sector has made participation of people working in energy industry a crucial factor for promoting organizational and societal sustainability goals at an individual as a responsible citizen of a country and as also as a responsible employee of an organization. Energy related companies are in a position of empowering their employees to embrace energy efficient behaviours, that will help in improving operational efficiency and more general climate goals (IEA, 2021). However, for effective employee engagement carefully planned incentives that address social, professional, and financial motivators. Programs like utility cost reductions and energy efficient bonuses have shown effectiveness at encouraging employees to embrace sustainable practices (Gillingham et al., 2018). Moreover, programs such as rewarding people with employee credits for reducing energy consumption that can be redeemed for rewards and personal benefits is cited as successful strategy (Allcot and Rogers, 2014). As an extension of workplace energy related goals, renowned organizations such as Google and Microsoft have adopted cost sharing systems for home solar installations to promote employee renewable energy practices (Hess and Sovacool, 2020). Additionally, recognizing people for their efforts in implementing practices of energy saving, cyber security is a powerful motivator. Features in games like leader boards and badges boost participation by appealing competitiveness, good competition and collaboration among people (Hamari et al., 2014). Providing real time feedback and practicing interventions through technology significantly improves energy related behaviors (Darby, 2006).

However, the REDISET project also identified several challenges faced by professionals in public and private energy-related organizations, including both cyber and non-cyber experts, when engaging in the energy system. One major issue is that cybersecurity responsibilities are often perceived as an additional workload on top of existing job duties. Another challenge is the limited or outdated knowledge among employees who have been in the same role for over a decade, making it difficult for them to adapt to evolving industry demands. Additionally, a general lack of motivation to learn further hinders engagement. Different individuals require different forms of motivation, such as financial incentives or additional time off, and the absence of personalized incentives makes it challenging to encourage active participation. The participation from people

could be limited because of wider reasons based on organizational, technological, behavioral, systematic challenges. Employees often lack awareness regarding their roles and impact of participation in energy systems. Same is highlighted as employee's ability to participate in complex energy systems is often limited due insufficient knowledge (Thøgersen, 2017). Due to high competition and changing markets organizations may prioritize short term financial yields over long-term energy efficiency investments. These kind of differences in actions towards energy efficiency and sustainable practices make it difficult for employees working in the organization to focus on energy related goals (Frederiks et al., 2015). Additionally, employees may find it difficult to understand advanced technologies such as smart grids, AI, IoT in energy systems because of lack of sufficient training (Fischer, 2008). Also, if employees participate in energy initiatives with their existing job, they may feel overburdened and see it as responsibilities (Deci and Ryan, 1985).

Employees may also have restrictions in implementing or adopting any form of innovative energy solutions, if they are working in companies with restrictive energy regulations and policies (Miller et al., 2015). There is a big investment involved in training, technology adoption or behavioral changes to evolve with the digitalized energy systems, people may think it as a financial burden (Frederiks et al., 2015). Due to ongoing geopolitical turmoil, the acquiring of materials and resources for new technology could face supply chain disruption. The digitalized systems are based on technologies that are dependent on real time data for decision making and optimization. Feeding outdated and poorly organized data or incomplete data will lead to poor decision making (Frederiks et al., 2015).

2.2.2 Digital habits and anticipated cyber security awareness and knowledge levels

The REDISET project findings highlight several key aspects regarding technology use and decision-making within the energy system. To effectively perform in the energy system, the segment relies on various technologies, including smart appliances and other digital tools. The usage of these technologies is typically confined within workplace boundaries set by the employer. Additionally, near-field communication (NFC) is commonly used for operational tasks. Psychological factors also influence technology use, as some employees may use their work phones for personal purposes, which can lead to accidental data storage on personal devices, or use their personal phone or e-mail to bypass cyber security restrictions that make their work process difficult. The segment's choices are primarily driven by financial considerations and data availability, shaping how they acquire the necessary supplies and resources for their work.

People in the role of employees use digital tools to facilitate their tasks of data analysis, energy management, and storage of large amount of data on cloud solutions. IEA (2021)

highlights that people use machine learning tools and energy management platforms to improve efficiency and predict system behaviors. Digital tools help organizations to establish successful remote controlling and monitoring, improve flexible operations (Hess and Sovacool, 2020). Employees use collaboration tools such as Microsoft Teams, cloud-based project management platforms. For cross department coordination and data sharing real time data sharing platforms play crucial role, for example IT and OT people (Thøgersen, 2017). This segment needs technologies that enable renewable integration, enable real time monitoring, collaboration tools, cyber security tools, and automated equipment. For example, smart appliances are part of an ecosystem to control and monitor energy usage, reduce waste and consumption (IEA, 2021). Another example is tracking renewable energy credits to make sure emissions are within asked limits (KPMG, 2020). During the REDISET project people with different experiences discussed that based on the people with different roles involved in energy organizations that can vary from a third-party contractor, helper, cleaner to an assembler to an engineer it can vary in between level 0 to level 1. During the REDISET project it emerged that basic knowledge should be at least level 2 for the people working in energy related organizations.

The reasoning why this segment would need the check list and manual was discussed with different stakeholders. The checklist and manual would need to be a "one spot for all" to keep people updated at least at a basic level about market trends, new technologies, and needed skills. It would also act as a tool for learning for the people who are working in the industry for their respective roles and will foster culture of preparedness. The manual acts as a standard protocol that simplifies the complexity of cybersecurity, additionally it expands to people at all levels – from IT engineers to assemblers, executives, contract people. According to National Institute of Standards and Technology (NIST) people with high awareness has less chances of making human error. It can help in fast response times with a standard step by step approach at the time of breach. A study was conducted by the Ponemon institute revealed that organizations with established incident response plans tends to take 48% less cost to recover and address any breach. Case study of colonial pipeline ransomware attack, 2021 reflects on that might be downtime during the ransomware attack could have been downsized and reduced the amount of losses. (Insurica, 2024)

2.3 Policymakers and market regulators

Energy policies are shaped by a diverse range of stakeholders, including legislators, energy producers, consumers, environmentalists, and trade associations, each with distinct priorities and interests (Kanna, 2023). In Finland, the Energy Authority serves as the national market regulator, overseeing licensing and regulatory functions while promoting the use of renewable energy, emission reductions, energy efficiency, and the

overall operation of the electricity and gas markets. Additionally, it plays a key role in advancing both Finnish and European energy and climate policies (Finnish Energy Authority, 2024). Findings from the REDISET project indicate that energy policymakers and market regulators operate as decision-making bodies that engage in both fast-paced and slow-paced decision-making processes. Fast-paced decisions address rapidly evolving issues such as data security, accuracy, and integrity, which have a direct impact on the flexible electricity market and law enforcement. In contrast, slow-paced decisions pertain to regional and sector-specific regulations that require long-term strategic planning. Regulatory bodies must also stay informed about industry standards and best practices such as standards from for instance International Organization for Standardization (ISO), National Insititute of Standards and Technology (NIST) and International Electrotechnical Commission (IEC) that act as standardization bodies for the energy sector. While keeping themselves up to date to these standards, policy makers and market regulators should also be constantly adapting to evolving cybersecurity needs. Furthermore, REDISET project findings highlight that policymakers and market regulators play a crucial advisory role, providing guidance to decision-makers such as members of the European Parliament. Their expertise ensures that legislative and regulatory frameworks remain aligned with the dynamic challenges of the energy sector.

2.3.1 Drivers and barriers in participating in the energy system

The primary objective of energy policies is to guide development toward sustainability goals and decarbonization, maintain market stability by ensuring a secure energy supply, and enhance the interconnection of energy networks (EU, 2024b), while also overseeing market actors at the local level (Finnish Energy, 2024). During the project work, it was observed that market regulators and policymakers play a crucial role in promoting sustainability goals, fostering continuous learning, and ensuring that top-tier expertise exists in the energy field. The incentives to participate in the energy system align with the responsibilities required to keep it operational. At the core of policymaking is the need to secure a stable and safe energy flow, which is essential for societal stability (EU, 2024b). This was also recognized during the project, with an added emphasis on enhancing the sustainability of the current system. Geopolitical instability has further elevated national security as a key consideration in policymaking. Russia's influence in the Baltic and Northern European regions affects the development of the Nordic energy system (Salonen & Kivimaa, 2024). Interviews conducted by them occurred in Finland, Estonia, and Norway and revealed that the perceived threat from Russia influences policymaking, particularly in Estonia. The presence of NATO's defense center in Estonia was also noted as a relevant factor. The interviews (Ibid, 2024) highlighted that the Nord Pool system reflects the risks associated with global energy networks and is closely tied to regional governance. While Russia was the most frequently mentioned security concern in Finland,

it was referenced less often than in Estonia. Additionally, Finland's open society was identified as a potential risk, as its reliance on trust-based open data policies creates vulnerabilities, particularly concerning the exposure of critical infrastructure locations.

Interestingly, it seems that many actors in Finland believe they are in charge of the country's security (Salonen and Kivimaa 2024), with committees and other bodies identified as part of energy security governance. Still, the ministry of economic affairs and employment—which is in charge of energy policy—was mentioned as the primary organization in this respect. Additionally, as new types of cyber-technical systems are integrated to the traditional energy system (Breitschopf et al., 2023) and the demands are changing in the markets, the decision-making processes need to be faster. This might be challenged by what could be perceived as tight-knit silos and conservative security viewpoints, along with a total lack of central coordination. (Salonen & Kivimaa, 2024) During the project work, it was observed that socio-political factors significantly impact the energy market. For example, Russia's influence has prompted swift measures to stabilize electricity prices, some of which have faced later criticism. Additionally, unexpected situations, such as flaws in Norway's spot market, have required immediate intervention from policymakers.

2.3.2 Digital habits and anticipated cyber security awareness and knowledge levels

The governmental duties are increasingly being digitalized, with terminology such as eGovernance being launched (Misuraca & Viscusi, 2014). During project work, it was recognized that with the significant new cyber risks brought along by artificial intelligence, no "individual creativity" to solve problems is allowed, and only pre-set secured tools such as hardware managed by IT Zero admin rights will be used. In other words, the usage of technology is seen to be very restricted and following specific guidelines for the policy and market regulators segment. It should be mentioned that there are several facets to the public-private partnership in national cyber security. Internet service providers (ISPs), global information companies (like Google, Facebook, and others), private cyber-security companies, human rights and civil rights advocates, law enforcement organizations, and civil society organizations all have different relationships with governments. However, the public-private partnership is frequently referred to as a single entity, ignoring this complexity, in both the pertinent policy documents and the cyber-security discourse at large (Carr, 2016). Thus, anticipating the level of cyber security awareness for this heterogeneous segment is also challenging. During project work, we assessed the level of cyber awareness for this segment to be between level 3 and level 4, and also stated that the role is rather passive in the form of following orders and being aware.

2.4 Workers of TSO, DSO and Generation, both cyber and non-cyber experts

The roles of TSOs (Transmission system operators), DSOs (Distribution system operators) and generation (power generation facilities) are to maintain secure and reliable infrastructures, operations, and data management. As digitalization has made the energy systems more decentralized, the roles are not only limited to specific key areas, but also to co-ordinate with each other, as well as cross border coordination (such as the Nord Pool and the Regional Security Centers) in accordance with the policies and frameworks. TSOs are responsible for managing the high voltage grids frequency and stability of the regional and national power system. This involves work roles such as grid operators, maintenance engineers and infrastructure designers. Digital systems in TSOs require to use big data techniques for monitoring and predicting any kind of disruption purpose which makes them vulnerable to cyber threats such as ransomware attack and data breaches (Mateska et al., 2021). Since TSOs operate under government guidelines their expertise is required in areas such as trans-border energy management, big area monitoring systems, and high levels of cybersecurity (CERRE 2016).

DSOs are responsible for distributing energy from transmission network to the consumer at a local level, but digitalization is advancing their role towards automation and data management. They also monitor energy consumption trends to notice any irregularity and to optimize the load distribution network (ENTOS-E, 2021). DSOs may contact external partners for cybersecurity practices because of their role limiting to local areas (CERRE, 2016). Many DSOs are small organisations, with amper personell for daily operation. Adding a cyber security awareness and competence in a small organisation might be challenging to keep the know-how up to date.

As discussed previously, data privacy and cybersecurity are critical areas in maintaining the stability of the energy system, and which need utmost attention because of increasing digitalized systems. Data privacy can be achieved by maintaining high levels of compliance with the general data protection regulation (GDPR) and non-disclosure agreements (NDA). Previous discussions and numerous studies highlight the importance of cybersecurity training to operation people and vulnerability of SCADA systems to the cyber-attacks (Mateska et al., 2021). Additionally, with the integration of IoT devices in DSO, data security measures are necessitated as per the organization's capability (ENTSO-E, 2021). New technologies such as blockchain and AI are area of interest, especially blockchain for peer-to-peer energy trading (Eurelectric, 2018). DSOs share critical data with TSOs to manage active power, prevent system imbalances, and support ancillary services (Energy system catapult, 2019). Overall, it can be said that responsibilities of TSO, DSO and generation can be multifunctional in areas of operations, security, reliability, continuity, and sustainability.

2.4.1 Drivers and barriers in participating in the energy system

During project work it was concluded that it is mandatory for these people to participate in the energy system. However, research puts attention to the relevance of flexible services in promoting involvement, integrating distributed energy sources (DER) to generate revenue by assisting grid operations such as maintain voltage stability, congestion monitoring (Eurelectric, 2018). As the energy system undergoes transformation with the integration of renewables, new digital technologies, and evolving policies and regulations, Transmission System Operators (TSOs), Distribution System Operators (DSOs), and energy generation professionals face significant challenges in navigating this increasingly complex, digitalized environment. Findings from the REDISET project highlight several key challenges in this transition. These include rising costs, intense market competition, and shifting geopolitical dynamics, which add pressure to energy organizations. Additionally, industry players must adapt to new methods of energy generation and the development of critical infrastructure, while also complying with evolving regional and sector-specific regulations and legislation. A shortage of skilled workers, particularly in cybersecurity, further complicates the transition, along with limited access to reliable information and data. The sector also faces technological disruptions, including the challenge of legacy systems that may not be compatible with modern digital infrastructure. Finally, decision-making risks, whether in policy development or political factors affecting energy markets, create additional uncertainty for stakeholders.

Advancing of the grid has introduced additional costs, research in this area reflects the type of costs associated with network reinforcements and implementation flexible solutions, for example energy storage systems (Marzband et al., 2023). There is a need of strategies to adapt optimal investment. Due to climate crisis and geopolitical factors, energy demand is also fluctuating which leads to need of evolved energy systems with technological advances that promote market designs with efficient participation by DERs and flexible services. For instance, Smartnet simulations highlighted issue of energy congestion, and an importance of mechanisms that support management of congestion as well as balance of services in transmission and distribution (Pagani et al., 2019). Other type of risks such as political uncertainty, delay in decision making and inconsistent policies are reasons for complications in work TSOs and DSOs (Papadaskalopoulos et al., 2022). Electricity based digital energy systems are highly susceptible to cyber-attacks, that emphasizes on necessary cybersecurity measures and training of workforce development (Yao et al., 2023). TSOs and DSOs need real time data exchange to operate with reliability for efficient grid operations. Bottleneck type situations may take place due to a centralized approach to data management, thus underscoring the necessity of balance between centralized monitoring and local autonomy (Zugno et al., 2022).

Traditional systems are the legacy systems with legacy technologies that make them vulnerable to cyber threats and a hinderance spot to the adoption of innovative solutions like microgrids and energy storage. To integrate renewables and to improve resilience of the grid, critical and modern infrastructures are important. To overcome these challenges, effective coordination between transmission and distribution network is required (Contreras at al., 2023). Operations between TSOs and DSOs often lack coordination in centralized frameworks. Modern hybrid models that distribute responsibilities between TSOs and DSOs need well defined operational and regulatory frameworks (Carreiro et al., 2022).

2.4.2 Digital habits and anticipated cyber security awareness and knowledge levels

TSOs and DSOs operation uses technologies such as geographic information system (GIS), Energy management system (EMS) and SCADA system. These tools are efficient for fault detection, load balancing, and grid monitoring. Additionally, advanced technologies such as PMU applications, blockchain and AI are being considered for secure data sharing and predictive analytics respectively in energy value chain. These developments make TSOs and DSOs energy efficient by allowing successful integration of renewable energy to the grid while also allowing management of DERs like wind and solar energy (Bytyqi et al., 2021). For secure data sharing between standardized platforms, it is emphasized to enable transparency and efficiency, one such example is project TDX- ASSIST that target to improve interoperability and standardize real time data exchange between grid operators (Bytyqi et al., 2021, Mayorga, 2020). R&D, consultancy and collaboration are important sources of data and information. Often energy operators practice simulation and predictive models to implement processes, for example virtual power plants, smart power cells for improved load, resource management and understanding (Mayorga, 2020, Bytyqi et al., 2021). During the project work it was discussed that currently this group has level 2 to level 3 understanding of security. Still, what would be expected from them would be to have level 3 to level 4.

2.5 Defense sector

According to Sabahattini et al. (2020) employees in the defense sector operate under pressure and should be able operate with situational awareness as they have limited time to complete difficult tasks. Defense workers are under pressure from international technological competition, and a country's ability to remain competitive rests on how well its industry can innovate and modernize. By combining various skills to innovate, defense workers prepare themselves for the exploitation of new technologies. The European Defence Agency (2024) states the enhancing of military capabilities, unit autonomy, and

operational resilience on the battlefield all depend heavily on energy efficiency. Samaras et al. (2019) state that the missions of armed forces around the world are fundamentally based on energy considerations. The authors (Ibid. 2019) claim that although concerns about clean energy have raised awareness of this relationship, the literature and media rarely specifically address the interplay between military and non-military energy issues. Additionally, the military has long assumed a leading position in the procurement and research and development (R&D) of particular energy technologies.

During REDISET work, the defense segment was stated to be defined by their work role in the energy system, which is about protecting the critical infrastructure from a total security perspective. This requires specific knowledge and solutions that are kept hidden from the public. The role of the total security aspect on energy security has focused on the security of the supply (Radovanović et al., 2017). This is supported by for instance by Winzer (2012), who suggests that the concept of energy security should be narrowed to energy supply continuity. In general terms, the defense segment needs to protect the energy system and thus have a plan b for emergency response. In the REDISET work, the responsibilities were also defined so that the defense sector provides relevant training to the policy makers and politicians regarding total security and energy, as well as prepared some critical data.

2.5.1 Drivers and barriers in participating in the energy system

Defense sites and activities requires energy for transportation, communications, heating, cooling, and lighting, among other energy-related services (Sahabattin et al., 2020). This segment provides defense and offense strategies in order to protect the system. Energy policy agendas are occasionally justified under the pretext of national security, claim Sivonen and Kivimaa (2024). Energy transition and securitization are paradoxical because transition means change, while security is a defensive idea that means keeping things as they are. When acquired values are not threatened, there is security. By changing the rules, actors, often state representatives, can label any issue as a security threat. This framing makes it seem urgent and justifies action. In securitization, prioritizing issues is key because calling something a security problem makes it one. According to Tvaronavičienė et al. (2020) the weakest spot in the implementation of Critical Infrastructure Protection (CPI) is the awareness and the training of the workers, fundamental for the development of newer solutions. During the project work the identified challenges in the energy system were the product safety throughout the supply chain starting from component safety to manufacturers processes.

2.5.2 Digital habits and anticipated cyber security awareness and knowledge levels

Research and innovation are in the core of defense strategies for instance in the European Defense Agency (2024). The REDISET project findings indicate that this sector needs to incorporate a cybersecurity-first mindset, as for instance data breaches have the potential to cause a lot of damage. Additionally, the internet access needs to be restricted in order to minimize exposure to cyber threats. The defense sector tends therefore to act as a closed network with aggregators and power plants participating in the market. This sector has strict access control policies, ensuring personnel only access data necessary for their role. During the project, it became evident that the reasons behind the procurement of specific technologies by the military and defense sector remain undisclosed, as such information is classified and not publicly accessible. However, according to Karaman and Aybar (2016) different nations have different approaches to cybersecurity and the understanding and management of cyberspace. Cyber-attack on critical infrastructure requires a combination of hacking and engineering knowledge to inflict maximum damages (Ang & Utomo, 2017). Thus, protecting critical infrastructure requires both information technology (IT) and operational technology (OT) expertise (Ang & Utomo, 2017). Krasznay and Hamornik (2019) argue that in the military context in cybersecurity practice, teamwork is just as crucial as the technical abilities that staff members must possess.

In the REDISET work the cyber security awareness level was estimated to be either 3 or level 4. The expected know-how was estimated to be on the same levels. According to Sivonen and Kivimaa's (2024) interviews regarding energy transition and securitization, cybersecurity emerged as a top priority for Finland's defense and security field within the total defense principle. To ensure the safety of the quickly evolving energy system, particular measures were considered to be required, as the energy sector was perceived to be lagging behind in cybersecurity legislation.

3 CORE CHALLENGES RELATED TO CYBER SECURITY IN ELECTRICITY BASED DIGITALIZED ENERGY SYSTEMS AND REDISET RECOMMENDATIONS

The academic literature highlights several key cybersecurity challenges in electricity-based systems, addressing both managerial and technical factors necessary to overcome them. Krause et al. (2021) propose that the key aim of cyber security management in the electricity sector is to secure the reliability and resilience of the system. The three fundamental objectives of cybersecurity are to ensure confidentiality, integrity and availability, also known as the CIA triad. In conventional cybersecurity practices, maintaining confidentiality and integrity is typically prioritized, even if it means potentially sacrificing some availability (Krause et al., 2021). However, as the needs of the energy sector are tied to maintaining the real-time functioning of the system, the dependence on availability requirements is a factor that needs to be considered. Although it has been argued that it is challenging to create one-size fits all recommendations for the sector (EECSP, 2017), the manual and the given recommendations aim to consider the factors that are energy sector specific: as availability needs to always be considered first, energy sector stakeholders also need specific measures to ensure integrity and confidentiality in the cyber realm.

The REDISET project has identified key challenges in cybersecurity management, categorizing them into cultural, behavioral, technical, and economic issues. Based on multidisciplinary research—including data from workshops, expert interviews spanning industry, government, and academia, as well as literature reviews—these vulnerabilities are recognized as the primary drivers of social-cyber-physical (Milevskyi et al., 2023) safety concerns within EBDES. Additionally, cyber-attacks stem from diverse motivations, ranging from financial fraud and personal gain to ideologically driven political objectives (Wang et al., 2020).

One of the most frequently cited examples of a successful cyberattack in the energy sector is the Ukraine power grid hack, which exploited multiple vulnerabilities. The attack began with phishing, allowing attackers to gain access and carry out remote sabotage. In the lead-up to Christmas 2015, they took full control of the Ukrainian power distribution grid's remote terminal units, manipulating breaker set points. As a result, critical breakers were opened, cutting power to approximately 225,000 customers for an extended period. A similar incident occurred in December 2016 when attackers once again used phishing to initiate remote sabotage. This led to a one-hour outage and disrupted energy delivery from a transmission station in Kiev, ultimately affecting 230,000 customers by opening breakers in substations. (Riggs et al., 2023; Wangen, 2015; Domovic, 2017).

The motivations behind cyber-attacks might vary significantly. Attackers can be classified as either insiders or outsiders, depending on whether they attempt to enter an organization from the outside or act from within (Han & Dongre, 2014). Wangen et al. (2015) claim that most cybercriminals are motivated by financial gain, particularly when launching extensive phishing attacks. On the other hand, similar to spear phishing, espionage targets specific individuals in order to obtain information, get ready for future attacks, or obtain negotiating leverage. This kind of attack necessitates specific knowledge, such as familiarity with the political and linguistic context of the target.

Based on the actor's motives or goals, cyberattacks are divided into four primary categories in literature. Hacking operations motivated by political propaganda, protest, or private motives like entertainment or self-validation are referred to as hacktivism. These attacks are frequently driven by ideology and are intended to support or contradict a political position, deal with social problems, or overcome personal obstacles. The goal of cyberespionage is to gain access to private company or government data by breaking into computer systems. Usually hidden, these operations are intended to support long-term strategic goals. The main driving force behind cybercrime is financial gain via unauthorized access to computer networks. Financial fraud, identity theft, and other types of digital exploitation for financial gain are all included in this category of non-violent criminal activity. As part of a larger digital warfare strategy, cyberwarfare, on the other hand, entails actions by a nation-state to interfere with or harm another country's computer systems or networks, frequently resulting in serious harm. There is also the idea of cyber retaliation, in which attackers have personal goals, like exacting revenge on a former employer. (Oueslati et al., 2019; Wangen, 2015; Domovic, 2017).

Thus, based on the project findings and academic literature, it can be concluded that the core cybersecurity challenges in electricity-based systems arise from multiple factors. Many different issues can ultimately lead to the same vulnerability—such as susceptibility to data breaches or a lack of cyber awareness within organizations—potentially resulting in significant harm. Figure 4. below presents a problem tree, a visual representation we used to analyze the core challenges in cybersecurity. In this structure, the roots represent the underlying causes, the trunk symbolizes the core challenges, and the branches illustrate the consequences, which can extend and spread. The problem tree analysis was used to systematically examine core cybersecurity issues, their root causes, and their broader consequences across the different segments.

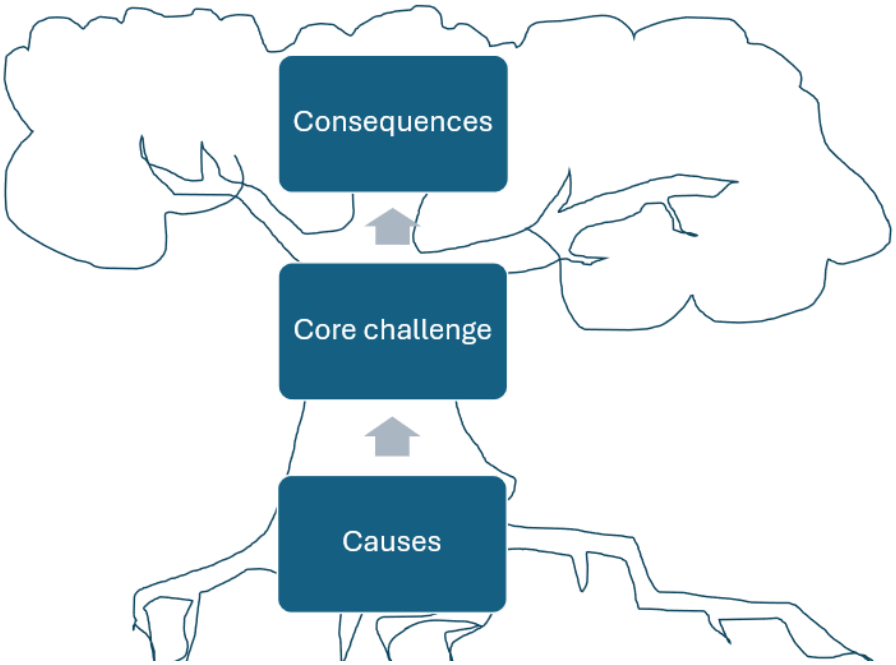

Figure 4. Problem tree.

The visual representations (see Fig. 4) help clarify how different challenges arise, identify their fundamental drivers, and illustrate their potential impact on the energy sector. Each challenge category is further analyzed using academic literature and a relevant cybersecurity case study. The insights from these analyses are then synthesized into research-based recommendations for addressing cybersecurity challenges within the energy sector.

This method was used to identify the key cybersecurity challenges within the EBDES framework. This chapter is organized around the main challenges identified during the REDISET project, along with research-based recommendations for addressing them. The challenges are categorized into four main groups: organizational cultural issues related to cybersecurity, behavioral challenges, technical challenges, and economic challenges presented in Figure 5 below.

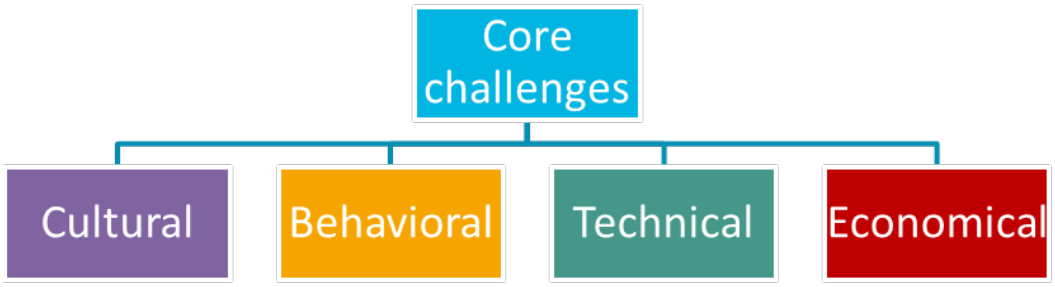

Figure 5. Identified core challenges of EBDES during REDISET Project.

The core challenges presented in the Figure 5. above identified by the REDISET group were complex and multifaceted and they were categorized into four main groups. The first category, cultural challenges, encompasses aspects related to organizational cybersecurity culture and strategic decision-making. The second category, behavioral challenges, focuses on individual behavioral factors that influence cybersecurity practices. The third category, technical challenges, pertains primarily to cybersecurity issues related to products and digitalization, rather than human factors. Finally, the economic challenges address financial constraints, including budgetary considerations that impact cybersecurity efforts.

All of the above mentioned core challenges are addressed in this chapter and these categories are elaborated upon further as shown in Figures 6 to Figure 17. However, it is important to note that the visual representation in the following Figures 6 to 17 follows a descending structure, in contrast to the problem tree diagram, where causes were depicted as roots and consequences as branches.

3.1 Cybersecurity cultural challenges

According to the definition of ENISA (2017) cybersecurity culture (CSC) within organizations encompasses the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values that individuals hold about cybersecurity and how these are reflected in their behavior when interacting with information technologies. It focuses on integrating information security into employees' roles, routines, and behaviors, embedding it as a natural part of their daily activities. According to Georgiadou et al. (2023), the cybersecurity culture in the energy sector varies, as employees possess different skill levels, leading to a disparity. Quader and Janeja (2021) further argue that the behavioural elements resulting up to attacks are the most vulnerable connection in an effective mitigation of cyber risks. (ENISA, 2017; Georgiadou et al., 2023; Quader & Janeja, 2021). The findings of the REDISET project, as illustrated in Figure 6. beneath, identified three primary aspects of cybersecurity-related cultural challenges.

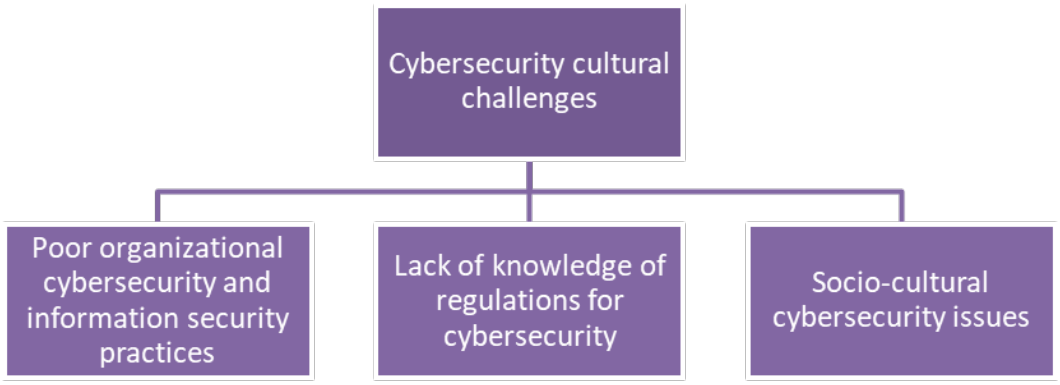

Figure 6. Cybersecurity cultural challenges grouped and identified during the REDISET project.

These challenges (see Fig. 6) include poor organizational cybersecurity and information security practices, a lack of knowledge regarding cybersecurity regulations, and socio-cultural cybersecurity issues. These key vulnerabilities were identified through the problem tree analysis. Each of these challenges is examined in greater depth in the texts below.

3.1.1 Poor organizational cybersecurity and information security practices

As visualized in Figure 7. beneath, REDISET research highlighted several critical issues stemming from weak organizational cybersecurity and information security practices. Key challenges included inadequate safety procedures, poor cybersecurity measures, biased or inaccurate information, subjective interpretations, limited communication between defense and energy production companies, the absence of a cohesive strategy, and insufficient safety habits.

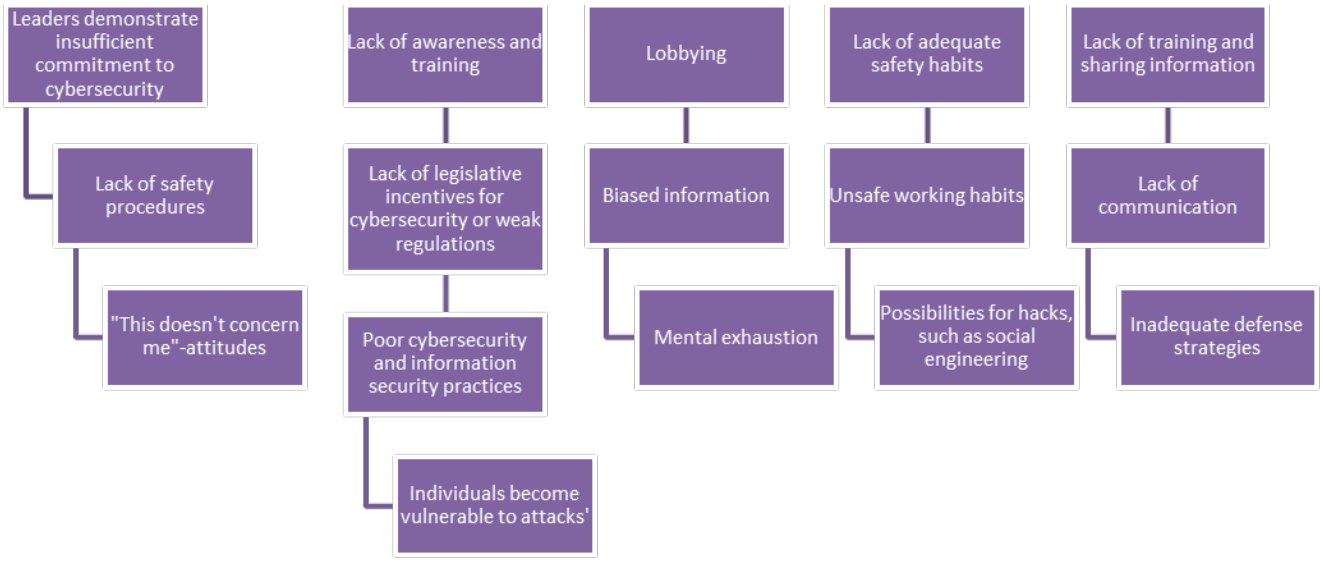

Figure 7. Poor organizational cybersecurity and information security practices.

Several underlying factors contribute to the challenges presented in Figure 7. Inadequate safety procedures often result from leaders showing indifference toward cybersecurity. Poor cybersecurity practices result from weak regulations, lack of incentives, and inadequate training. Lobbying efforts may lead to biased or inaccurate information, while inadequate training for policymakers in the energy sector, combined with limited knowledge-sharing between energy and defense personnel, hampers communication between these groups. These issues carry significant risks with potentially severe consequences. Weak organizational cybersecurity and information security practices can foster harmful attitudes, such as disengagement ("This doesn't concern me"), leaving individual prosumers more susceptible to attacks like social engineering and ransomware. Moreover, these vulnerabilities can cause mental fatigue, increasing the likelihood of errors, and contribute to the absence of a clear and effective defense strategy, jeopardizing the security of the entire energy system.

3.1.1.1 Recommendations for enhancing cybersecurity culture

A strong cybersecurity culture is essential for mitigating cyber threats and ensuring the resilience of organizations against evolving security risks. Cybersecurity culture encompasses not only technical defenses but also organizational practices, leadership engagement, employee awareness, and interorganizational collaboration. Table 2. in this section outlines key recommendations for enhancing cybersecurity culture, focusing on leadership involvement, the implementation of security protocols, employee training, and fostering collaboration within and beyond the organization.

Table 2. Recommendations for enhancing cybersecurity culture.

Key Area	Recommendations
Strengthening leadership and engagement	- Leaders should actively promote cybersecurity awareness and involve employees in discussions. - Organizations should implement "detective, protective, and preventative controls" and consider "offensive defense" strategies such as red teaming and penetration testing. - Organizations should prioritize securing employee commitment to mitigate insider threats. - Corporate accountability should be emphasized in cybersecurity management. - Regular security briefings should be conducted to increase awareness and engagement at all levels.
Developing and enforcing safety procedures and protocols	- Organizations should implement cybersecurity standards to reduce cyber threats. - Standards help define compliance requirements and establish performance benchmarks. - External certification and audits ensure adherence to standards. - Cybersecurity frameworks provide guidelines, while standards define specific steps for compliance.
Providing training and awareness programs	- Organizations should offer frequent and updated cybersecurity training. - Employees need continuous learning to stay informed about emerging threats. - Cyber defense activities should align with organizational culture and values. - Phishing simulations should be conducted regularly to reduce susceptibility.
Encouraging collaboration	- Organizations should foster teamwork to enhance cybersecurity defense. - Sharing threat intelligence across organizations strengthens defense strategies. - Collaborative cybersecurity incident management enhances response capabilities. - Organizations should work together to better understand and respond to cyber threats. - National Cyber Security Centers provide support in case of cybersecurity incidents

The Table 2. above presents key recommendations for strengthening cybersecurity culture, highlighting four critical areas: leadership involvement, security procedures, employee training, and collaboration. Each of these areas plays a significant role in establishing a security-conscious work environment that can proactively defend against cyber threats.

The next chapters will provide a deeper analysis of these recommendations, exploring best practices, relevant research, and implementation strategies. By understanding and applying these principles, organizations can foster a more robust cybersecurity culture and reduce the risks posed by cyber threats.

3.1.1.2 Strengthening leadership and engagement in cybersecurity

Distance work has become more common since the pandemic, but because employees frequently use their personal devices to download software and access company data, cybersecurity has also grown in importance and is a problem that organizations need to consider. Workers' ignorance of cybersecurity can have serious consequences, such as making them easily distracted, anxious, and worn out, which increases the risk of security incidents. However, according to, for instance Triplett (2022), employees are not solely to blame. In addition to being held responsible for enforcing cybersecurity policies, cybersecurity leaders have an obligation to make sure that company policies are being followed. Leaders also need to be better prepared to discuss these issues with employees in an effective manner. Leaders can encourage the development of positive awareness and improve human behaviors regarding cybersecurity by involving employees. (Triplett, 2022)

Ho and Gross (2021) claim that in addition to establishing "detective, protective, and preventative controls", organizations should be prepared to use "offensive defense." Offensive cybersecurity refers to proactivity in security measures using the same methods as attackers use in order to strengthen the network (IBM, 2024). Methods vary from red teaming, penetration testing and assessing vulnerabilities. However, Quader and Janeja (2021) assert that most undetected cyber-attacks stem from insider threats. To mitigate these risks, organizations must prioritize securing employee commitment and fostering loyalty to uphold cybersecurity policies and safeguard digital assets. Without trust and reliability among employees, a company’s digital resources become highly vulnerable to various cyber threats. (Quader & Janeja, 2021)

In order to increase employee trust and reliability, corporate accountability should play a larger role in cybersecurity management (Quader & Janeja, 2021). Although leaders are accountable for cybersecurity in organizations increasingly due to legislative iterations such as with new cybersecurity legislation, should this be prioritized strategically

(Triplett, 2022). Regular security briefings among the staff should be prioritized to increase awareness and engagement in all organizational levels (Triplett, 2022).

3.1.1.3 Developing and enforcing safety procedures and protocols

A key component of cyber-security management is creating and implementing safety procedures and protocols; using standards is perceived as one method to do this. Cybersecurity standards are designed to assist organizations in safeguarding their cyber operating environments by defining specific technical procedures and sets of practices. These guidelines offer a framework for evaluating an organization's operational and management procedures in relation to predetermined standards. According to Heras-Saizarbitoria and Boiral (2013), standards define the ideal performance or quality level that an organization must achieve in order to be deemed compliant, as well as the lowest acceptable level. An external third party provide a certification for a company so that the certified company can show compliance. After certification, audits can be used to externally evaluate the business's operations to make sure they meet the standards. (Syafrizal et al., 2020; Heras-Saizarbitoria & Boiral, 2013; Finnish Standards Association, 2024).

Cybersecurity standards typically fall into two main categories: information security standards and information security governance standards. Selecting a standard or guidelines should be based on the particular needs of the organization in order to be certain they suitably meet the requirements of the business, according to Syafrizal et al. (2020).

If a company already has a cybersecurity framework, the possible implementation of a standard is seen appropriate to be aligned to that framework. Cybersecurity frameworks individually do not define what steps need to be taken, but rather act as general recommendations that encompass a number of components or areas that companies may apply. Cybersecurity standards, on the other hand, clearly outline the measures that comply with the standard and establish the measures in a chronological order, highlighting what is expected to be done throughout the process. For example, Antunes and Tate (2022) advise that if a business is implementing a framework, it should provide an overall framework and methodology along with a description of the implementation, evaluation, and scope processes. (Taherdoost, 2022; Syafrizal et al., 2020; Antunes & Tate, 2022).

3.1.1.4 Providing training and awareness programs

Abrahams et al. (2024) recommend constant training and improvements are achieved by holding frequent and modern cybersecurity training sessions for staff members. It is essential to continue learning as the threat landscape changes. Regular updates can maintain staff members updated about arising threats, novel attack vectors, as well as the best practices according to the authors. (Abrahams et al., 2024). Quader and Janeja (2021) emphasize that comprehensive training to educate employees about cyber threats is essential for safeguarding a corporate network. This ongoing effort ensures that employees remain informed about emerging threats and understand how to protect themselves and the organization. Without adequate training and awareness, internal IT environments become highly susceptible to attacks, providing opportunities for hackers. For example, interactive voice response (IVR) or phone phishing attacks often exploit this lack of awareness. When employees cannot distinguish between legitimate and phishing emails, they risk unintentionally creating vulnerabilities that compromise IT systems. (Quader & Janeja, 2021)

According to Ho and Gross (2021) cyber defense activity in organizations necessitates that a system's objective characteristics are considered significant by the participants. This involves things like common identity, beliefs, and opinions that are shaped by culture and society. Therefore, in order for awareness campaigns and other activities to succeed it is crucial for participants to adopt new technology and processes with a positive attitude. In cybersecurity, progressive learning is crucial, and tool knowledge is developed gradually. (Ho & Gross, 2021) It has been noted that for instance with phishing attack simulations, the more often they happen, the less amount of people fall as victims (Chatchalermpun & Daengsi, 2021)

3.1.1.5 Encouraging collaboration

Teamwork is crucial at all stages of cyber security defense, and losing team processes has a negative impact on the effectiveness of cyber defense as a whole (Rajivan & Cooke, 2017). By encouraging collaboration, organizations can together work on the whole supply chain cybersecurity. According to Solansky and Beck (2021), information exchange is essential when cooperative interorganizational action is needed to combat cybersecurity threats. The inclination to share knowledge with other companies that hold the resources to assist in combating the threat should be encouraged by managers of organizations that respond to cybersecurity threats. The integrated interorganizational initiatives are more likely to be undertaken by cybersecurity threat-related organizations that are open to exchanging information. (Solansky & Beck, 2021).

Oriola et al. (2021) argue that, large-scale information security devices, a buildup of security expertise, and the vast amount of incident data are all advantages of collaborative-based cybersecurity incident management (Oriola et al., 2021). For instance, Settanni et al. (2017) claim that in order to gain a more comprehensive understanding of the current cyber threat landscape, organizations must collaborate to share security-related information. This will allow them to gain fresh insights into their infrastructures and respond promptly if needed. (Settanni, et al. 2017).

Organizations can also contact se national cyber security centre in case of help needed: in Finland it is National Cyber Security Centre Finland (National Cyber Security Centre Finland, 2024).

3.1.2 Lack of knowledge of regulations for cybersecurity

During project work two main issues were identified. The first was that "No one follows our guidelines and recommendations". If organizations struggle to comply with laws, guidelines may have little impact. The second issue is a lack of knowledge regarding cybersecurity regulations. These are presented in Figure 8 below.

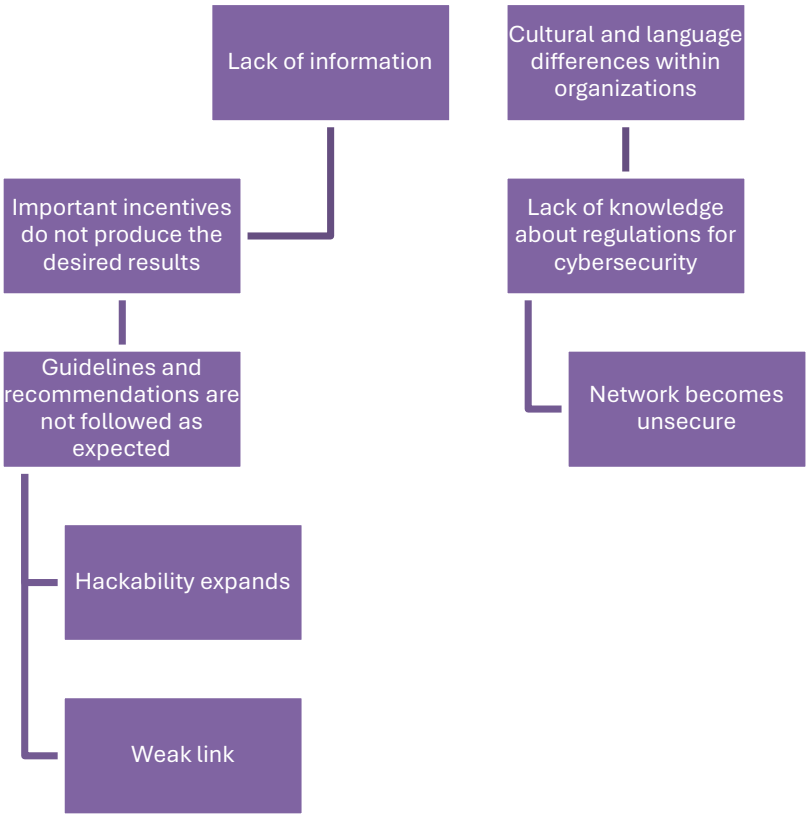

Figure 8. Lack of knowledge of regulations for cybersecurity.

Contributing factors to the issues presented in Figure 8. include insufficient information, poorly implemented incentives that fail to achieve desired outcomes, and misunderstandings due to language and cultural differences. These issues are concerning as they ultimately lead to a less secure network.

3.1.2.1 Recommendations for addressing the lack of knowledge of regulations for cybersecurity

Ensuring cybersecurity resilience requires a structured approach that integrates governance, awareness, and compliance within organizations. The Table 3. presents key REDISET recommendations, outlining essential actions to strengthen cybersecurity practices. These recommendations focus on three core areas: governing cybersecurity through contracts, enhancing awareness about legislation, and adapting training materials to align with regulatory requirements.

Table 3. Recommendations addressing the lack of knowledge of regulations for cybersecurity.

Recommendation Area	Key Actions
Governing cybersecurity through contracts	- Raising cybersecurity awareness in the supply chain through contractual agreements. - Combining relational and contractual governance for better results. - Including cybersecurity risk management clauses in vendor contracts. - Implementing time-based mitigation measures in contracts. - Using a vendor rating system after compliance assessments.
Enhancing awareness about legislation	- Launching a Code of Conduct for Cybersecurity to define appropriate behavior.
Adapting training material	- Developing training materials that cover cybersecurity legislation, including GDPR, NIS2, and DORA, to ensure compliance.

3.1.2.2 Governing cybersecurity through contracts

The project recommendations for addressing lack of knowledge of regulations for cybersecurity include governing cybersecurity through contracts to raise awareness in the supply chain, enhancing awareness about legislation, and adapting training material (see Table 3.). Insufficient client-vendor relationship governance is a key reason many IS outsourcing projects fail to deliver expected benefits. Previous studies have often

treated relational and contractual governance as alternatives, suggesting that a contract may reduce the need for a trust-based relationship and vice versa. It is also argued that combining both approaches can provide additional benefits. Boyson (2014) outlines several steps in the supplier contract lifecycle to improve cybersecurity governance. The first step in pre-contract coordination is incorporating provisions in vendor contracts that require cyber risk management. A formal contract should define time-based mitigation measures to be implemented midway through the contract lifecycle. After compliance is assessed, a vendor rating system is used to evaluate performance. (Boyson, 2014)

3.1.2.3 Enhancing awareness about legislation

Enhancing awareness about legislation involves increasing the understanding of cybersecurity laws and regulations among stakeholders. It is considered crucial for ensuring compliance and fostering a culture of security within organizations. This could include launching a code of conduct for cybersecurity to establish clear guidelines for appropriate behavior in cybersecurity practices. A well-defined code of conduct helps in setting standards and expectations, thereby promoting ethical and responsible actions among cybersecurity professionals. (Macnish & Van der Ham 2020).

3.1.2.4 Adapting training material

Adapting training materials to encompass cybersecurity legislation is crucial for ensuring organizational compliance. This process involves the development of comprehensive training programs that address key regulations, including the General Data Protection Regulation (GDPR), the Network and Information Security Directive (NIS2), and the Digital Operational Resilience Act (DORA).

The GDPR is a significant regulation governing data protection and privacy within the European Union. It establishes stringent standards for the processing and storage of personal data, thereby ensuring that organizations implement robust measures to safeguard individuals' privacy (Tikkinen-Piri et al., 2018).

The NIS2 Directive aims to achieve a high common level of cybersecurity across the European Union. It mandates that member states enhance their cybersecurity capabilities, streamline reporting obligations, and enforce stringent security measures to protect critical infrastructure (Vandezande, 2024).

The DORA focuses on the digital resilience of financial entities within the EU. It requires these entities to manage ICT risks effectively, report major ICT-related incidents, and

ensure the operational resilience of their systems against cyber threats (Clausmeier, 2023).

By integrating these regulations into training materials, organizations can ensure that their employees are well-informed about legal requirements and best practices for cybersecurity, thereby enhancing overall compliance and security posture.

3.1.3 Socio-cultural cybersecurity issues

The identified core problems include internal organizational "cyber cultural deterioration", characterized by a lack of motivation and awareness, and vandalism, such as intentional damage to equipment (e.g., incidents where Teslas were vandalized on the street). Contributing factors include overly complex rules and expectations that are difficult to understand, overwhelming tasks, and the notion of "no free lunches"—where strict security measures may hinder motivation. Additionally, value-based decision-making (e.g., anarchism/Trumpism, anti-PV, and anti-EV movements) counters the green movement. Figure 9 depicts the identified socio-cultural challenges.

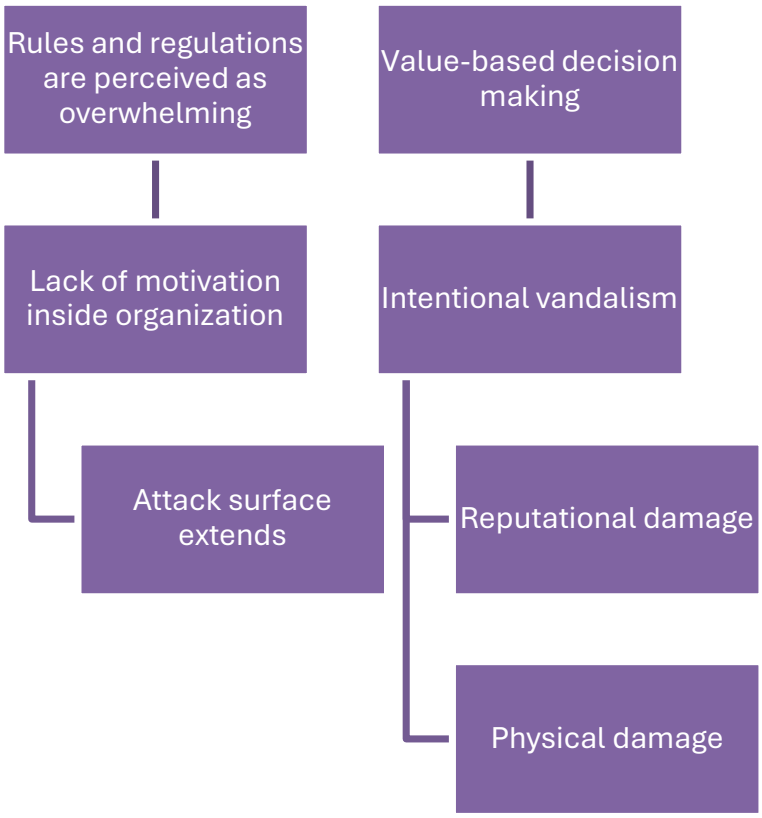

Figure 9. Socio-cultural cybersecurity challenges.

The core problems presented in Figure 9. are concerning because their effects could include a larger cyber-attack surface, reputational damage, and physical damage to equipment, such as PV systems. Cyber awareness can be key cultural factor in an organization, which can help protect from cyber threats (Quader & Janeja, 2021).

3.1.3.1 Recommendations for addressing socio-cultural cybersecurity challenges

The social and cultural dimensions of cybersecurity, including human factors, remains critical for fostering a safe and resilient cybersecurity culture (Georgidau et al., 2023). Following Table 4. presents suggestions for how to solve socio-cultural challenges related to cyber security.

Table 4. Recommendations for addressing socio-cultural cybersecurity challenges.

Recommendation Area	Key Actions
Increasing public awareness for cybersecurity and green technologies	- Educate the public on cybersecurity threats and the importance of green technologies. - Implement cybersecurity awareness programs, such as those from CISA. - Address ideological resistance by promoting informed decision-making.
Simplifying procedures and creating step-by-step guides for incident response	- Reduce complexity in cybersecurity procedures to enhance employee motivation and compliance. - Develop step-by-step guides to make incident response processes clear and actionable. - Regularly review and update these guides to ensure they align with current threats and needs. - Use NIST's four-step incident response cycle: preparation, detection and analysis, containment, eradication, and recovery as a framework.
Enhancing communication	- Foster a culture of cybersecurity awareness through effective communication. - Conduct regular training sessions tailored to different levels of employee understanding. - Implement phishing simulations, workshops on threat recognition, and secure password guidance.

3.1.3.2 Increasing public awareness for cybersecurity and green technologies

Enhancing public understanding of cybersecurity and the importance of green technologies can help mitigate intentional damage and resistance stemming from ideological opposition. Implementing comprehensive cybersecurity awareness programs, such as those advocated by the Cybersecurity and Infrastructure Security Agency (CISA), can educate individuals on potential threats and the significance of sustainable practices (CISA, 2024). By increasing awareness, organizations and individuals can develop a stronger sense of responsibility in protecting both digital and physical assets.

3.1.3.3 Simplifying procedures and creating step-by-step guides for incident response

Overly complex rules and expectations can overwhelm employees, leading to decreased motivation and potential security oversights. Simplifying cybersecurity procedures and providing clear, step-by-step incident response guides can make protocols more understandable and actionable. Regularly reviewing and updating these guidelines ensures they remain practical and aligned with current needs. The National Institute of Standards and Technology (NIST) outlines a four-step incident response cycle—preparation, detection and analysis, containment, eradication, and recovery as well as post incident recovery that can serve as a foundation for developing these guides (Young, 2020). Ensuring that employees have access to easy-to-follow security procedures enhances compliance and reduces the likelihood of errors.

3.1.3.4 Enhancing communication

Effective communication within an organization fosters a culture of cybersecurity awareness and responsiveness. (Georgidau et al., 2023). Regular training sessions tailored to different levels of understanding help ensure that all employees are aware of potential threats and best practices. These programs can include simulated phishing attacks, workshops on recognizing suspicious activities, and guidance on secure password practices. By improving communication and training efforts, organizations can reinforce cybersecurity awareness and ensure that employees are better equipped to identify and respond to security threats. (Assante & Tobey, (2011).

3.2 Behavioral challenges

Cybersecurity behavior describes individual cybersecurity vulnerabilities that can relate to for instance double digital identity as well as attitudes towards cybersecurity,

inconsistent security practices and being preoccupied with other tasks. Quader and Janeja (2021) suggest that our personalities shape how we respond to real-life scenarios, influencing our behavior in various situations. Similarly, in the cyber world, our inherent traits guide our reactions to digital stimuli. For instance, our fundamental nature determines whether we choose to click on a link embedded in an email, open an attachment, or interact with a link on a website we are browsing. Figure 10. shows the core challenges related to individual human behaviour.

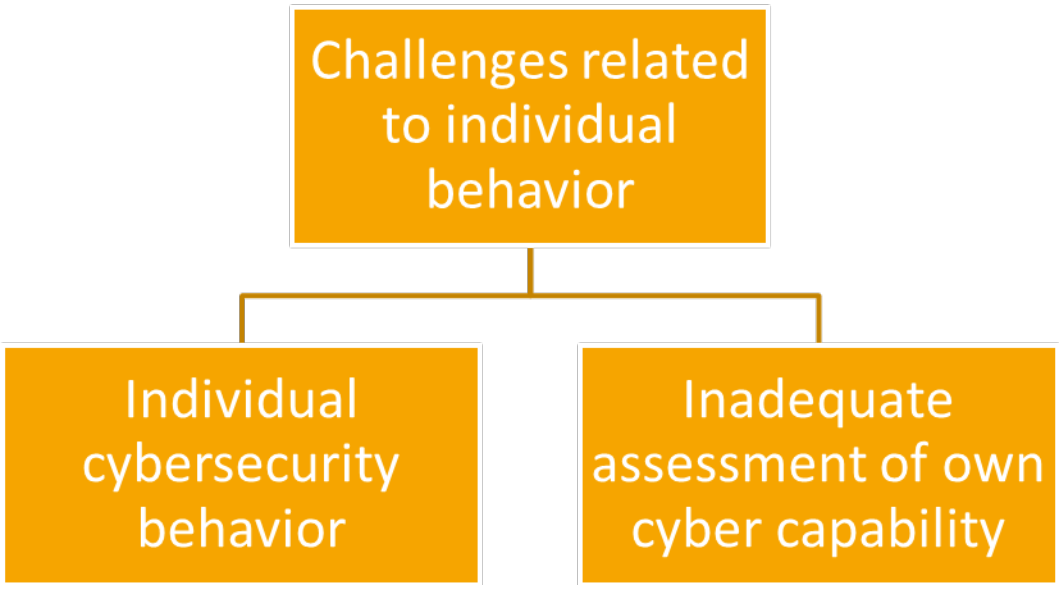

Figure 10. Challenges related to individual behavior.

In a 2015 study, Wangen highlight that human vulnerability is a key target in for instance espionage efforts. Their analysis reveals that almost all known attack vectors involved social engineering, typically through spear phishing, where attackers trick users into actions like opening email attachments or using infected USB sticks. Soykan & Bagriyanik, (2020) claim that the motives behind SMiShing attacks are to harvest personal information such as email, address, name, and banking information. However, it is also stated that the motives vary with every target and situation. (Wangen, 2015; Soykan & Bagriyanik, 2020)

Our personalities determine our behavior in real-life situations and how we respond to them. Like in real life, when we encounter a stimulus online, we often respond according to our basic nature. For example, we may decide whether or not to click on a link in an email, open the attachment in the email, or click on a link on the webpage we are currently viewing (Quader & Janeja, 2021). In a literature case, a worm exploited Iran's nuclear program in 2009-2010, and no Iranians had knowledge about it. Stuxnet Cyber Warfare had an adverse effect on a large number of people, which was between 250,000 to 500,000. (Quader & Janeja, 2021).

3.2.1 Individual cybersecurity behavior

Individual cybersecurity behavior refers to the actions, attitudes, and decisions that individuals make regarding cybersecurity practices, which can significantly impact an organization's overall security. Quader and Janeja (2021) argue that the weakest link in effectively preventing cyber threats is human behavior, as certain actions can unintentionally facilitate cyberattacks. Distraction, ignorance, curiosity, disregard for security policies, and a lack of awareness about cyber threats are among the behaviors that can lead to significant harm. The authors (Ibid. 2021) highlight that while cybersecurity and physical security share many similarities, individuals tend to prioritize the latter. For example, a phishing simulation test conducted by Holm et al. (2013) demonstrated how employees' choices directly impacted the company's cybersecurity. In the experiment, employees received two phishing emails, and observations revealed that many attempted to access a blocked server, possibly due to curiosity or ignorance. The study also found that context-specific phishing attacks were not necessarily more effective than generic ones, as the former could attract more scrutiny. Additionally, misconceptions about email spoofing were identified; for instance, one employee underestimated the risks of malware, assuming that the primary danger was only the compromise of a high-level email account. Figure 11. elaborates upon the core problems related to individual's cybersecurity behavior.

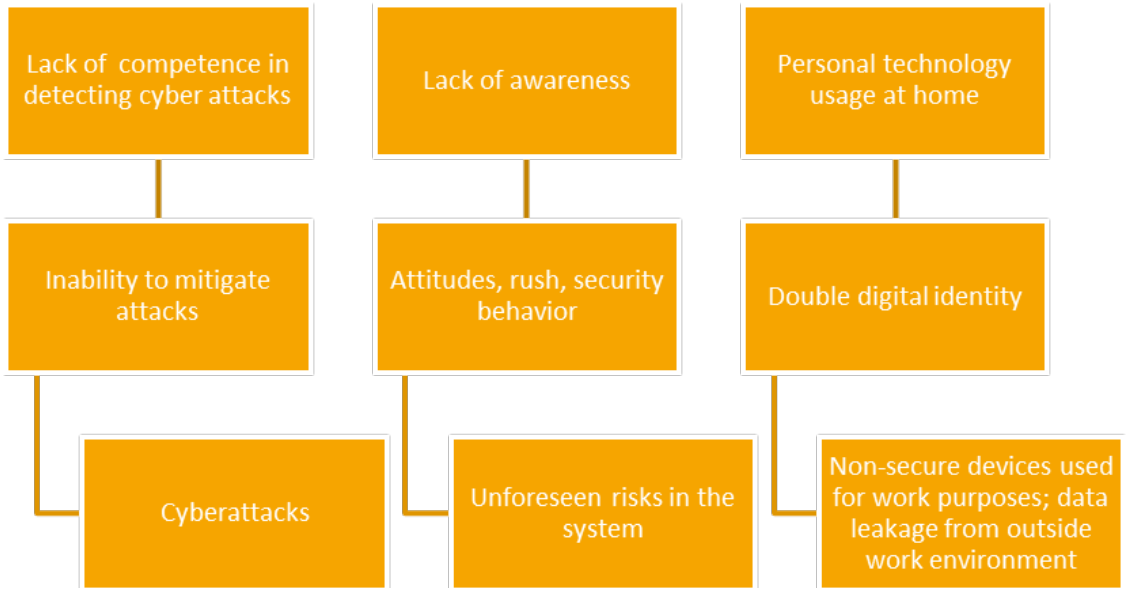

Figure 11. Individual cybersecurity behavior.

The core problems identified in Figure 11. above include a lack of understanding and competence in detecting cyber-attacks, human behavior issues such as attitudes towards cybersecurity, inconsistent security practices, being preoccupied with other tasks, and challenges in managing double digital identities. The causes were linked to factors such

as a lack of awareness, human psychology, personal technology usage, and less secure habits at home. These issues were deemed problematic due to their potential effects, including blackouts, system-wide vulnerabilities, human-related cybersecurity risks, the use of unsecured devices for work, and data leaks from outside the work environment.

3.2.1.1 Recommendations for addressing individual cybersecurity behavior

Human behavioral aspects have frequently been identified as the most vulnerable link in cybersecurity (Pollini et al., 2022). Quader and Janeja (2021), through an analysis of 43 cyber-attack case studies from the past decade, identified four key human factors contributing to these incidents: ignorance, negligence, misconfiguration, and deceit. Out of the four main human factors, ignorance and negligence are the two human behaviors that appear to be linked to most of the cyber threat. As an example, the adoption of bring your own device (BYOD) policies and the increasing use of employee-owned mobile devices to access corporate networks have introduced new vulnerabilities, requiring additional layers of cybersecurity. (Quader & Janeja, 2021). Following Table 5 gives recommendations for how to solve possible cyber security risks caused by individual behaviour.

Table 5. Recommendations for addressing individual cybersecurity behavior challenges

Recommendation Area	Key Actions
Improving awareness	- Educate individuals about the dangers and threats posed by cyberspace and their susceptibility. - Inform people of the negative effects of cyber threats and how attackers may target victims. - Provide guidance on recognizing cyber threats and their warning signs. - Raise awareness of existing security measures, including tools, policies, regulations, and best practices. - Encourage individuals to take proactive steps to mitigate cyber threats. - Emphasize the value of cybersecurity and individual responsibility in maintaining security.
Single sign-on (SSO) and identity management & data encryption techniques	- Implement authentication methods that allow users to verify their identity securely. - Reduce security risks associated with password reuse and identity theft. - Use alternative authentication methods like Privacy-Enhancing Attribute-Based Credentials (P-ABCs), SSO, and individual user certificates. - Enable SSO to allow users to access multiple systems with a single authentication, improving security and efficiency. - Enhance productivity and reduce administrative risks by managing authentication centrally.
Secure remote work policies	- Recognize that individual values influence ISP (Information Security Policy) compliance, especially in remote work environments. - Customize cybersecurity programs to account for different compliance behaviors between remote and onsite workers. - Address the "my house, my rules" attitude by designing security policies that align with employees' values. - Motivate remote workers with flexible and innovation-driven security policies. - Emphasize that employee opinions are considered in security policies, reinforcing the idea that compliance enhances freedom.

3.2.1.2 Improving awareness

Raising awareness about cybersecurity threats is essential in ensuring individuals understand the dangers they face in cyberspace. People need to be informed about the negative effects of cyber threats and the potential actors involved, including how they operate and the resources they may exploit. Providing knowledge on how to recognize cyber threats and their warning signs is crucial, as is making individuals aware of the security measures currently in place to combat these threats. This includes tools, policies, procedures, guidelines, standards, regulations, laws, strategies, and best practices. Encouraging proactive action by implementing security measures can help mitigate risks. Educating people on the importance of cybersecurity and their role in maintaining it further strengthens overall security efforts (Chaudhary et al., 2022).

3.2.1.3 Single sign-on (SSO) and identity management & data encryption techniques

User authentication is a fundamental aspect of cybersecurity, ensuring that individuals can securely verify their identity when accessing various services. Frederiksen et al. (2019) highlight that authentication typically requires a username containing confidential information, with passwords serving as a primary method of verification. However, using the same username and password across multiple service providers poses significant security risks. Password reuse, combined with a compromised provider, can quickly lead to identity and financial theft. Additionally, traditional username-password authentication methods make it difficult to share verified attributes such as age or place of residence. Alternative authentication methods, such as Privacy-Enhancing Attribute-Based Credentials (P-ABCs), Single Sign-On (SSO), and individual user certificates, offer more secure and flexible solutions. Radha and Reddy (2012) explain that SSO enables authorized users to access multiple software systems or applications with a single authentication action, eliminating the need to log in separately to each system. This approach not only enhances security but also reduces administrative burdens and improves user productivity by simplifying authentication processes.

3.2.1.4 Secure remote work policies

The implementation of secure remote work policies is another crucial factor in strengthening cybersecurity. Torres and Crossler (2024) identify personal values as a key predictor of adherence to information security policies (ISP). Their study indicates that remote workers display varying levels of compliance compared to onsite employees, emphasizing the need for customized cybersecurity programs that align with individual values. Organizations must design cybersecurity initiatives that motivate remote

employees while addressing the "my house, my rules" mentality toward security. Workers with more conservative values are more likely to comply with policies established by managers and authorities, whereas those with a greater openness to new experiences may require a different approach. The authors argue that remote work environments are better suited for individuals who thrive on innovation and flexibility. Businesses can benefit from understanding that these employees are motivated by freedom and adaptability. Consequently, cybersecurity communications and policies should highlight the importance of employee input in shaping security measures while reinforcing that compliance ultimately enhances their autonomy.

3.2.2 Inadequate assessment of own cyber capabilities

The core problems identified during the project work include a lack of knowledge about the potential consequences of cybersecurity threats, legacy thinking, and an incorrect assessment of capabilities, summed up by the idea, "We don't know what we don't know." Figure 12. showcases the main challenges and their causes related to assessment of cybersecurity.

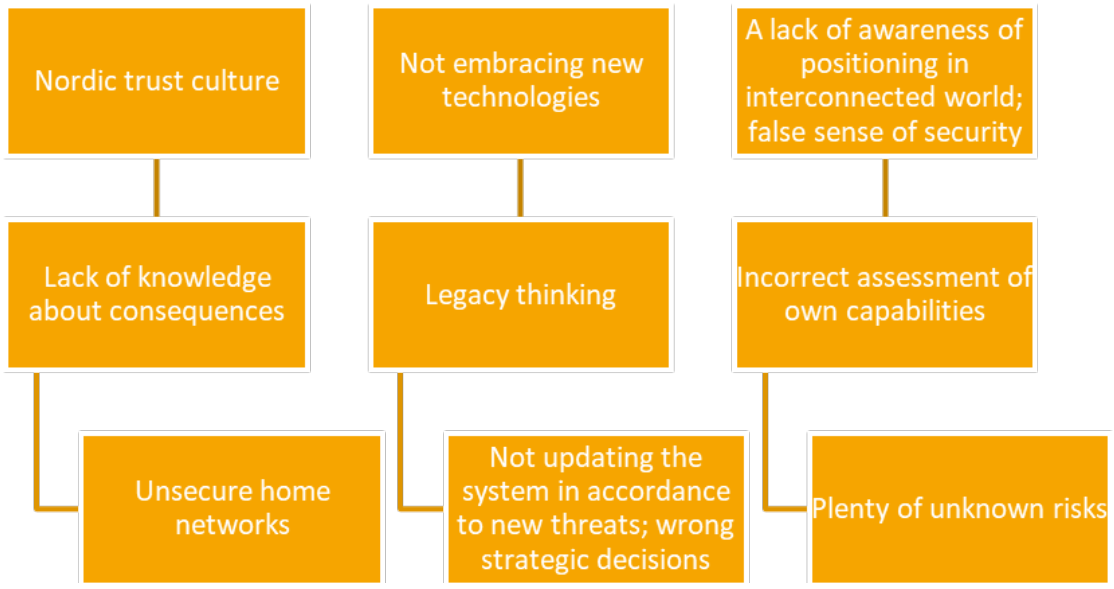

Figure 12. Inadequate assessment of own cyber capabilities.

The causes of these issues presented in Figure 12. include the Nordic value of trust, which makes people more susceptible to scams and attacks due to a tendency to trust others too easily. Additionally, there is a resistance to embracing new technologies, often driven by a lack of young leadership. Another contributing factor is the belief that "we are safe" because of compliance with safety regulations, while assuming that other countries are

worse off, without recognizing the interconnectedness of global cybersecurity risks. These are considered problems since the possible effects include unknown hacks, unsecure home networks as well as not updating the systems adequately.

3.2.2.1 Recommendations for addressing users own cybersecurity capabilities

Earlier research by Georgidau et al. (2023) reveal substantial variations amongst the assessment of own cybersecurity capabilities amongst participating workforce in the energy sector, showcasing that there are still actions to be taken to secure critical infrastructures. Table 6. shows REDISET recommendations to solve issues related to assessment of capabilities.

Table 6. Recommendations for addressing challenges regarding cyber skill assessments.

Recommendation Area	Key Actions
Encouraging proactive cybersecurity mindset	-Shift from reactive to proactive cybersecurity strategies by fostering a culture of continuous learning and threat anticipation. -Promote scenario-based training and cyber resilience exercises to prepare for unexpected threats. - Establish cybersecurity resilience as a key priority in organizational strategies. -Encourage executive leadership to invest in advanced threat intelligence and real-time monitoring systems.
Strengthening critical thinking and digital skepticism	-Address legacy thinking and misplaced trust by integrating cyber-critical thinking programs. -Conduct real-world phishing simulations to help individuals recognize social engineering tactics. - Encourage a questioning mindset and teach individuals to verify digital interactions before trusting them. - Develop interactive training modules to simulate cyberattacks and improve critical awareness among employees.
Leadership renewal and generational inclusion	-Support younger leadership involvement in cybersecurity and digital transformation strategies. - Encourage mentorship programs that bridge traditional leadership with emerging cybersecurity perspectives. -Implement structured leadership training in cybersecurity decision-making.

Recommendation Area	Key Actions
	-Foster cross-generational collaboration to ensure cybersecurity policies reflect both experience and innovation.
Enhancing technological adaptability	- Reduce resistance to new technologies by demonstrating the benefits of emerging cybersecurity solutions. -Promote cybersecurity innovation programs to incentivize organizations to adopt new technologies like Zero Trust security models. -Encourage businesses to upgrade outdated security infrastructures. -Provide financial incentives and funding opportunities for businesses that implement cutting-edge cybersecurity technologies
Moving beyond compliance to active cybersecurity management	-Address the false sense of security from regulatory compliance by encouraging active cybersecurity risk management. -Encourage continuous vulnerability assessments and penetration testing beyond regulatory requirements. -Foster cross-border cybersecurity collaboration to acknowledge the interconnectedness of global cyber risks. -Develop industry-wide cybersecurity benchmarking to measure and improve security postures across organizations.

3.2.2.2 Encouraging proactive cybersecurity mindset

Proactive cybersecurity strategies involving continuous learning and threat anticipation can help organizations foster a strong cybersecurity culture. This can be achieved by regularly updating employees on the latest cybersecurity trends and potential threats. Also, investing in advanced threat intelligence and real-time monitoring can help in anticipating, identifying and mitigating possible threats before they can cause damage. (TechAdvisory.org 2025).

Scenario-based training and cyber resilience exercises can be done by conducting scenario-based tabletop exercises to simulate real-world cyber incidents. Such exercises might be helpful in testing and improving incident response plans, enhancing communication and collaboration between teams, and identifying gaps in current

processes (Burgett, 2024). Also, the implementation of regular cybersecurity drills to ensure that all employees are prepared for potential cyber threats (CISA 2024).

Cybersecurity resilience should be considered as a key priority, and also making sure leadership is involved in cybersecurity initiatives. A resilient infrastructure that is built around cyber security is not only about protecting but also recovering from possible attacks. One step is to encourage executive leadership to invest in cybersecurity by demonstrate the potential business impact of cybersecurity threats. This includes showing how advanced threat intelligence and real-time monitoring can prevent significant financial and reputational damage. Also, it is important to consider positioning cybersecurity investments as a competitive advantage that can enhance customer trust and brand reputation (Tetteh and Otioma 2024, Dinha 2025).

3.2.2.3 Strengthening critical thinking and digital skepticism

Cyber-critical thinking programs offered by various universities and other learning institutes are good opportunities for upskilling key actors' knowledge and capabilities. (CISA, 2024). Phishing simulations such as for example the IBM's phishing simulations test an organization's ability to recognize and respond to phishing attacks. They mimic real-world phishing attempts to educate employees on identifying and avoiding such threats (Badman, 2023).

To have a questioning mindset in cybersecurity it is important to learn effective questioning techniques**.** Asking the right questions is crucial for identifying potential risks and vulnerabilities. Effective questioning helps uncover hidden risks and enhances strategic decision-making and incident response (Institutedata.com 2024). This is also related to transforming cybersecurity mindsets as recognizing and changing how we think about security can lead to more positive outcomes and a healthier security environment (Tyson, 2023).

3.2.2.4 Leadership renewal and generational inclusion

Involving younger leaders can be an effective strategy for navigating cybersecurity disruptions. Forward-thinking CEOs see cybersecurity threats as opportunities to innovate and set their organizations apart. By taking a proactive stance, they can turn these threats into drivers of growth and long-term success (Dinha, 2025). This approach also ties into generational inclusion in cybersecurity. Recognizing the unique challenges and strategies relevant to different generations can help organizations bridge the digital generation gap, fostering effective communication and mutual understanding (Laczi & Póser, 2025).

Mentorship programs are recognized as an effective method for enhancing the skills and advancing the careers of especially upcoming professionals in cybersecurity. These programs focus on developing competencies in leadership, communication, and work-life balance (Wang and Sbeit, 2020). Similarly, structured leadership training is crucial for the professional development of managers and decision-makers in the field (Burrell, 2019).

Cross-generational knowledge sharing leverages the strengths of diverse perspectives to improve collective cybersecurity awareness and resilience. Promoting intergenerational collaboration and knowledge exchange within organizations can effectively bridge the cybersecurity awareness gap and enhance overall security practices (Dkaidek and Rashid, 2024).

3.2.2.5 Enhancing technological adaptability

To reduce resistance to new technologies it is important to demonstrate the benefits of emerging cybersecurity solutions (Vishik et al., 2013). Benefits of emerging cybersecurity solutions might come from artificial intelligence (AI) as it enhances cybersecurity by predicting and responding to threats in real-time, analyzing vast amounts of data, and automating routine security tasks (Zhang et al., 2022). Another example of evolving technology is quantum-safe security which requires adopting post-quantum cryptography to protect against future threats (Rawal and Peter, 2022).

By promoting cybersecurity innovation programs, it is possible to incentivize organisations to adopt new technologies, such as Zero Trust security models. The Zero Trust Principles is a security framework that requires strict identity verification for every access request, minimizing the risk of breaches by assuming no inherent trust (Dhiman et al., 2022). This also relates to the importance of upgrading outdated security infrastructure to enhance overall cybersecurity and efficiency. There are hidden costs of outdated IT infrastructure as older systems can lead to increased maintenance costs, security vulnerabilities, and decreased productivity. In some cases, upgrading old security systems with modern, eco-friendly technology can enhance performance, reduce environmental impact, and align with corporate social responsibility objectives. (Rajwan et al., 2020, Jha, 2023, Riggs et al., 2023). On a policy and national security level, it is important to provide financial incentives and funding opportunities for businesses that implement cutting-edge cybersecurity technologies. (Gordon et al., 2015).

3.2.2.6 Moving beyond compliance to active cybersecurity management

Active cybersecurity risk management involves transcending the false sense of security provided by mere regulatory compliance, thereby promoting a more dynamic approach to managing cybersecurity risks (Cremer et al., 2022). This approach necessitates continuous vulnerability assessments and penetration testing to identify and mitigate risks that extend beyond regulatory requirements (Bennouk et al., 2024).

Furthermore, cross-border cybersecurity collaboration is essential to address the interconnectedness of global cyber risks, particularly in sectors such as energy, where international cooperation is prevalent (Casino et al., 2024). Developing industry-wide cybersecurity benchmarking practices is also crucial for measuring and improving security postures across organizations (Chernenko et al., 2022).

3.3 Technical challenges

The convergence of the long-isolated OT and IT systems has brought numerous benefits to the energy sector, e.g., improved optimization, enhanced data analysis, automated decision making, etc. However, it has also introduced a range of cyber threats to the OT domain and consequently the energy sector. According to Quader and Janeja (2021), Advanced Persistent Threat (APT) attacks are often associated with insufficient technology adoption, inadequate training, and weak security policies. These factors, if not well-addressed can result in medium to significant financial losses. While cyber awareness is important to address these issues, it is not sufficient on its own; rather, effective cybersecurity requires proper training and the implementation of appropriate technologies. The technical problems in EBDES are diverse and increase in complexity with the increasing dependence on digital systems. These interdependent systems are now vulnerable to unpatched systems, outdated software, and misconfigurations, to name a few. Figure 13. depicts core technical challenges related to cyber security and human behavior.

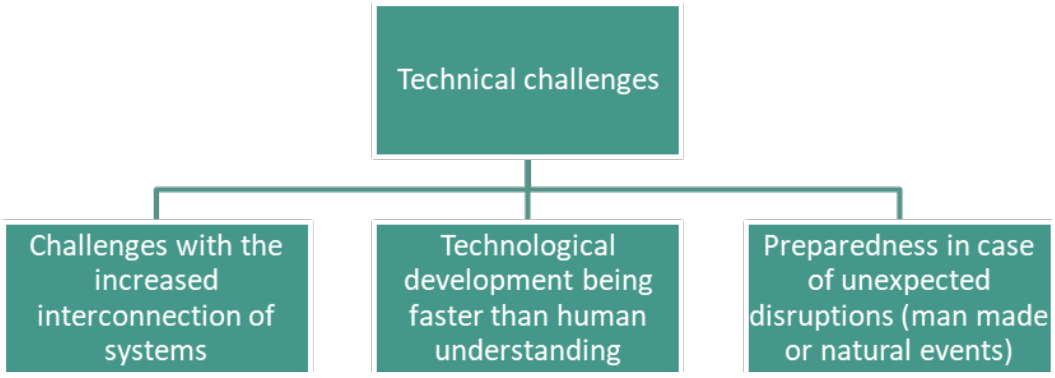

Figure 13. Technical challenges identified during the REDISET project work.

As examples of the issues presented in Figure 13., research by Althouse et al. (2021) and Mitropoulous et al. (2020) highlights the systems' weaknesses in terms of security, with missing basic security features that lead a lack of or delay in patching, thus giving attackers an opportunity to exploit vulnerabilities. At the same time cyber-attacks are now more sophisticated because of the use of AI to plan malware and phishing campaigns (Smith and Jones, 2022). An increased number of ransomware attacks to demand cryptocurrency payments in exchange for decrypting data has also been reported in recent years (Wu et al., 2020).

3.3.1 Challenges with the increased interconnection of systems

The identified problems include the hackability of interconnected products in smart homes, which increases cybersecurity threats due to system interconnectivity, such as ICT compatibility issues. The monopoly of certain providers creates a single point of failure, compounded by a lack of cybersecurity knowledge. Possible causes include devices like phones that continuously listen and store data, as well as reliance on licensed products and centralized systems. Figure 14. shows key challenges related to the increased interconnectedness of systems.

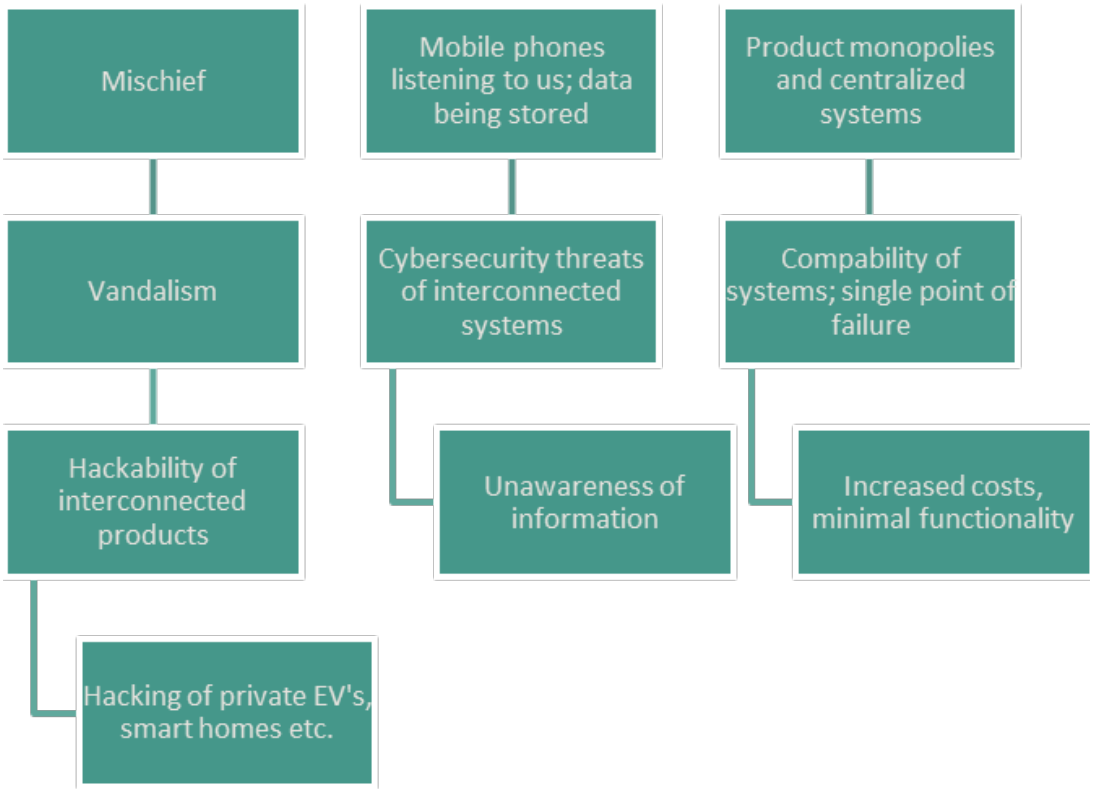

Figure 14. Challenges with the increased interconnection of systems.

These issues presented in Figure 14. are problematic because they could lead to consequences like hackers damaging photovoltaic (PV) systems, shutting down electricity, breaking into homes, increasing costs, reducing functionality, making recovery more difficult, and spreading misinformation through fake news.

As an example, Goudarzi et al. (2022) discuss the challenges of IoT-Enabled Smart Grids. IoT-enabled smart grids enhance energy demand management in the 21st century by offering real-time control and monitoring of grid components, facilitating the integration of distributed renewable energy, and enabling live communication of tariff information and energy consumption between consumers and service providers. Additionally, they collect grid statistics to support smarter decision-making. However, these grids face challenges such as increased cybersecurity vulnerabilities and exposure, stability and reliability issues, concerns over energy consumption and efficiency, and operational and economic risks from potential cyber adversaries. (Goudarzi et al., 2022).

3.3.1.1 Recommendations for addressing cyber challenges related to increased interconnection of systems

Naqvi et al., (2021) introduce a case study centered on smart grids within the realm of cyber-physical systems, asserting its' novelty as the first work pertinent to usable security

within CPS and smart grids. They argue that due to safety concerns linked to specific services such as advanced metering infrastructure (AMI), it is crucial to address the cybersecurity aspect. Moreover, they emphasize that security considerations should extend beyond discussions of network vulnerabilities, attack vectors, and countermeasures, highlighting the importance of incorporating the human facet of security services. This human facet encompasses the human element in the utilization and implementation of security services, encompassing factors such as cognitive abilities, behavior, and decision-making processes.

Recognizing the integral role of humans in the security system, Naqvi et al. (2021) stress the significant impact of human actions and decisions on the effectiveness of security measures. Consequently, they advocate for the essential consideration of the human element, e.g., end-users, in designing and implementing security services to ensure usability, effectiveness, and efficiency. This approach, commonly known as usable security, aims to integrate security and usability to develop systems that are both secure and user-friendly. Table 7. presents a set of recommendations to address challenges caused by the interconnectedness of systems.

Table 7. Recommendations for addressing the challenges regarding the increased interconnection of systems

Recommendation Area	Key Actions & Justification
Network segmentation	- Implement network segmentation to divide IT and OT systems into smaller, isolated subnetworks. - Limit access rights and communication channels to prevent unauthorized access. - Use mechanisms such as Access Control Lists (ACLs), Virtual LANs (VLANs), and AAA protocols. - Separate IT and OT networks to prevent cascading effects from cyberattacks. - Consider "Zoning models" based on connectivity requirements, frequency, and trust levels. -Leverage Software-Defined Networking (SDN) for fine-grained and dynamic segmentation.
Ensure compatibility between different devices	- Ensure security standardization and adherence to communication protocols to mitigate interoperability risks. - Avoid fragmented systems caused by non-compliance with universal standards. - Replace outdated protocols with modern security procedures to minimize vulnerabilities. - Implement fast detection and isolation of compromised devices to enhance network security. - Ensure safe data exchange while minimizing misconfigurations.
Usage of intrusion detection systems and firewalls	- Deploy firewalls as the first layer of defense to monitor and control traffic. - Utilize Intrusion Detection Systems (IDS) to detect and respond to cyber threats proactively. - Protect against attacks like advanced persistent threats (APT), zero-day vulnerabilities, and ransomware. - Adopt a layered defense approach to mitigate financial losses, reputational damage, and data breaches.
Usage of cybersecurity frameworks	- Implement security frameworks such as the NIST Cybersecurity Framework to strengthen cybersecurity governance. - Use a risk-based approach to prioritize cybersecurity measures. - Incorporate technical solutions like IDS and firewalls to enhance resilience. - Continuously improve cybersecurity strategies to counter emerging threats in the energy sector.

3.3.1.2 Network segmentation

The modern energy infrastructures are digitalized with the integration of IT and OT systems, which function by interconnected elements such as smart grids, IoT- enabled devices (such as sensors, drones but also digital substations), and cloud-based platforms. These interconnected systems are vulnerable to threats that can compromise sensitive data, potentially disrupt power supply and can also undermine the reliability of critical infrastructure. These systems currently create a wide area attack surface for cyberattacks due to the integration of IoT devices, smart meters, and advanced control systems (Shahzad et al., 2018). Additionally, because of their dependency on low latency communication systems to perform decision making in real time, such systems are vulnerable to denial-of-service attack (DoS) (Yan et al., 2018). Another aspect is the critical infrastructure itself where any kind of attack can have cascading effects, leading to potential large-scale societal disruptions (Amin et al., 2013). To limit these effects and unauthorized access, network segmentation can be an effective solution that divides network into smaller isolated subnetworks. Segmentation provides layered protection against cyber-attacks by limiting access rights and communication channels. It relies on mechanisms such as dividing Access Control Lists (ACLs), Virtual LANs (VLANs), and AAA protocols (Kim et al., 2020). For instance, having separate networks for IT and OT systems (Miller and Rowe, 2012). Such an approach "Zoning models" that could be founded on connectivity requirements, frequency and trust levels can also be considered for separate IT/OT systems in smart grids (IEC 62443-3-2, 2018). Trends such as Software-Defined Networking (SDN) feature fine-grained and dynamic segmentation (Jararweh et al., 2020).

3.3.1.3 Ensuring compatibility between different devices

Ensuring compatibility between interconnected heterogeneous devices is one of the most crucial cybersecurity challenges, because of their design and specifications. Therefore, security standardization and adherence to communication protocol is significantly important to mitigate risks associated with interoperability. Fragmented systems could result from non-compliance and lack of universal standards where devices and equipment from different suppliers may not operate and communicate seamlessly, thus exposing the system to vulnerabilities (Lu et al., 2020). Systems are often exposed to threats because of devices built on outdated protocols operating within modern security procedures (Oliveira et al., 2021). Furthermore, compatibility implements fast detection and isolation of compromised devices, resulting in simplified network management (Liang et al., 2021). This allows safe exchange of data while minimizing vulnerabilities and misconfigurations (Yan et al., 2018).

3.3.1.4 Usage of intrusion detection systems and firewalls

With the rise of sophistication of cyber threats, energy systems must be always alert, thus, tools such as intrusion detection system (IDS) and firewalls are essential to safeguarding digital infrastructure. Firewalls act as the first face of defense in monitoring and controlling incoming and outgoing traffic. IDS on the other hand simultaneously detect and respond to potential threats. Attacks like advanced persistent threat (APT), zero-day vulnerabilities, and ransomware all need proactive measures to detect and mitigate attacks before any significant damage is reported (Conti et al., 2020). Research highlights the significance of layered defense from the realization that any intrusion to critical networks can cause financial loss, reputation harm, and data breaches. Few IDS are able to detect intrusions, such as network-based IDS, host-based IDS, rule-based IDS and anomaly-based IDS (Storm, 2025).

3.3.1.5 Usage of cybersecurity frameworks

Boeding et al. (2022) identify various cybersecurity threats to the power grid, such as denial-of-service attacks, malware, and physical attacks, which can compromise availability, integrity, and confidentiality, especially with the convergence of IT and OT. To counter these challenges, they recommend implementing security frameworks such as NIST Cybersecurity Framework, adopting a risk-based approach, and using technical solutions like intrusion detection systems and firewalls. Their research emphasizes the importance of robust cybersecurity governance in the energy sector, suggesting adopting industry standards and continuous improvement of strategies to enhance the sector's resilience against cyber threats. (Boeding et al., 2022).

3.3.2 Technological development is faster than human understanding of it

Regarding the fast pace of technological development, the identified problems included data leakage and inadequate data protection, with the lack of security updates leading to vulnerabilities and making it easier to install viruses on outdated software. AI-driven attacks – particularly using closed-source software – and issues with detecting vulnerable entry points and vital devices were also highlighted. Figure 15. shows the challenges related to the speed of technological development.

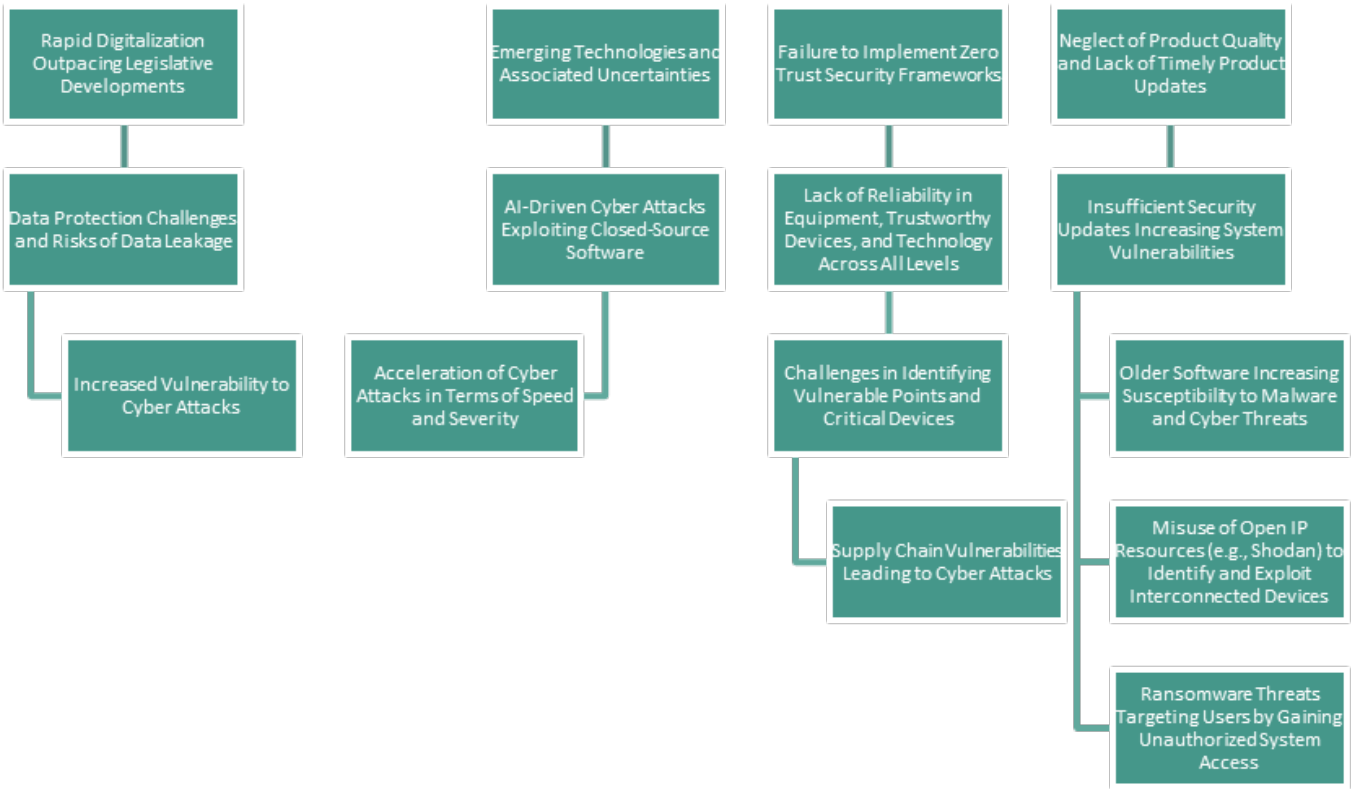

Figure 15. Technological development is faster than human understanding of it.

As depicted in Figure 15. above, contributing causes include the rapid pace of digitalization, legislation lagging behind technological advancements, the introduction of unknown new technologies, failure to implement zero-trust security models, and the lack of reliable, trustworthy devices and technology at all levels. These problems are concerning because they can lead to consequences such as ransomware attacks (where attackers gain access to systems and demand payment), exploitation of open IPs via tools like Shodan to identify and target interconnected products (e.g., video surveillance cameras, allowing cybercriminals to monitor individuals), faster and more severe attacks, and vulnerabilities in the supply chain.

3.3.2.1 Recommendations for addressing challenges related to the fast development of technology

Recent research describes the emerging, complex digitalised systems as socio-cyber-physical systems (Milevskyi et al., 2023) or cyber-physical-human systems (Bhandari et al., 2023). It pinpoints that the pace of technological development is forcing key stakeholders such as firms to develop cybersecurity governance programs that defne and promote the protection of an organisation's data, systems and networks (Hasan et al., 2021). Table 8 presents a collection of recommendations for keeping up to the pace of technological advances.

Table 8. Recommendations for addressing technical issues.

Recommendation Area	Key Actions
Applying zero-trust Model	- Implement a Zero Trust security framework where no entity (internal or external) is trusted by default. - Utilize network segmentation, least privilege access, and continuous verification to reduce attack surface. - Leverage technologies like blockchain to enhance authentication and data integrity. - Strengthen security with Identity Access Management (IAM), continuous monitoring, and threat detection. - Apply multifactor authentication and role-based access control to enhance system security.
Regular software updates and device reliability	-Ensure timely software updates to prevent vulnerabilities from outdated systems. - Conduct routine firmware and patch management to enhance device reliability. - Use automated update mechanisms to minimize human error and delay in critical security patches. - Implement device authentication and integrity checks to ensure systems remain uncompromised.
Strengthening cybersecurity protocols	- Conduct regular risk assessments and third-party audits to ensure cybersecurity measures align with global standards. - Integrate security requirements in vendor contracts to reduce supply chain risks. - Foster collaboration within the supply chain by sharing cybersecurity insights, data, and best practices. - Encourage supplier partnerships rather than transactional relationships to align cybersecurity interests across the supply chain.

3.3.2.1 Applying zero-trust model

Ongoing research highlights that interconnected systems are prime targets for attackers. A solution framework is based on the zero-trust paradigm, which assumes that no internal or external entity should be trusted by default. This framework brings into action segmentation, least privilege access, and continuous verification. Technologies such as blockchain are a recent area of research within this field. The company that introduced this term explains it as a strategy that believes all people, devices, and applications are not trusted until verified (Yeoh et al., 2023). While implementing the zero-trust model,

Identity Access Management (IAM), network segmentation, continuous monitoring, threat detection, securing communication channels and data, multifactor authentication, and role-based access control help in reducing the attack surface area.

3.3.2.2 Regular software updates and device reliability

Ensuring regular software updates and device reliability is essential in maintaining cybersecurity resilience. Interconnected systems remain highly vulnerable if software and firmware are not regularly updated. Updates are necessary to patch known security vulnerabilities and ensure that devices remain protected against evolving threats. Automated update mechanisms help minimize the risks associated with human error and delays in applying critical security patches. Additionally, device authentication and integrity checks play a crucial role in maintaining system security by verifying the authenticity of connected devices and detecting anomalies that could indicate a security breach.

3.3.2.3 Strengthening cybersecurity protocols

Risks related to cyber supply chain management can be reduced by different methods, such as risk assessments, reversed hardware cyber security investigations, third-party auditing, utilizing and requiring standards in contracts, and aligning interests and cooperating with stakeholders within the supply chain. Borenius et al. (2022) state that it is essential to decrease supply chain attacks, since buyers consider the general quality of the products and the cybersecurity measures of the suppliers, including safe development processes. According to Yeboah-Ofori and Islam (2019), supply chain parties should implement their security processes in accordance with international standards and conduct regular audits by third parties in order to guarantee appropriate control and mitigation methods in the cyber supply chain. Cooperating within the supply chain regarding cybersecurity issues has been deemed beneficial by multiple academic researchers. According to Kumar and Mallipeddi (2022), for instance, sharing data, resources, and profits or costs among the parties involved in the supply chain are examples of coordinating supply chain interests. Aichbauer et al. (2022) propose a modern approach to leadership in procurement, where suppliers are regarded as partners rather than just vendors.

3.3.3 Preparedness in case of unexpected disruptive events

Even though many cybersecurity threats are directly rooted in human behavior, problems such as technical malfunctioning and unpredictable weather, can lead to human errors

and thus vulnerabilities in digital connections. Figure 16. demonstrates two unexpected events that may cause challenges to the security of the energy system.

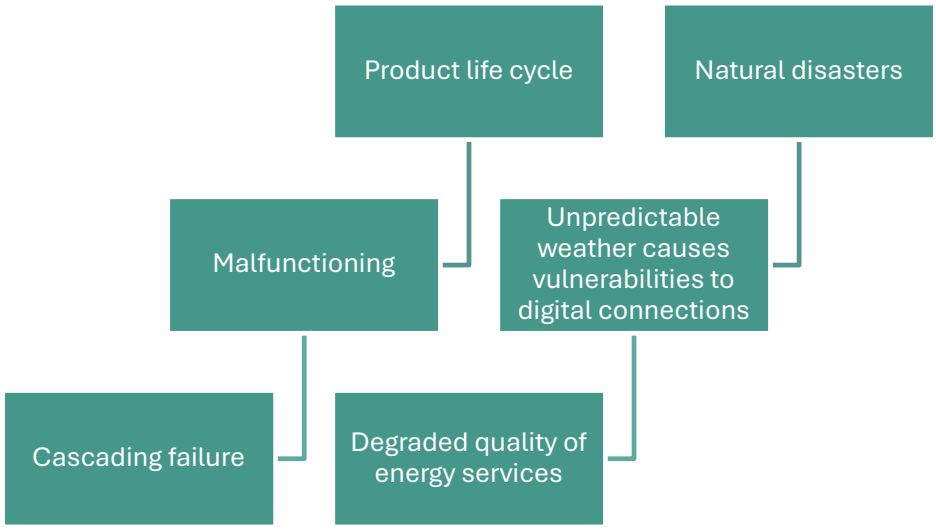

Figure 16. Preparedness in case of unexpected human made or natural events.

Causes behind the issues presented in Figure 16. include varying product life cycles and natural disruptions. These problems are concerning because they can result in cascading failures and degraded energy service quality. Preparedness in case of sudden failures is crucial for maintaining the balance of the energy system.

3.3.3.1 Recommendations for addressing preparedness to unexpected disrupted events

As complexity and the digitalisation of the energy system is progressing, the frequency of unexpected events will increase while the inertia in the system is shrinking, making it more sensitive to such disruptions with less time to act (Berg et al., 2024). Following Table 9. gives recommendations to how to handle unexpected disruptive events.

Table 9. Recommendations for addressing challenges of preparing to unexpected disruptive events

Recommendation Area	Recommendation
Opting for resilience and N-1 implementations	- Implement N-1 redundancy to ensure system reliability and mitigate failures. N-1 meaning that one component can fail without influencing the security of supply. - Use backup systems to prevent disruptions in case of component failure. - Enhance fault tolerance by designing systems with spare capacity to handle failures.
Performing segmentation and decentralization	- Divide networks into isolated segments to limit the impact of cyber incidents. - Apply decentralized architecture to prevent complete system failures. - Utilize n(n-1)/2 topology to interconnect critical network components, eliminating single points of failure.
Following minimum viable services approach	- Prioritize essential components to maintain security and continuity during failures. - Reduce system complexity by maintaining only necessary functionalities. - Ensure critical services remain operational under adverse conditions.

Opting for resilience and N-1 implementations, where redundancy is used to ensure reliability, is could be a solution to mitigate such situations, however if one component is affected it is likely to assume that the same component in the redundant branch is affected, so a manual operating back-up plan might be more efficient. Another approach is by ***performing segmentation, decentralization***, and using of n(n-1)/2 topology for connecting the most critical network components, thus avoiding any single point of failure. Furthermore, the concept of ***minimum viable services*** should be followed, prioritizing the most essential components to ensure continuity and security. (Carvallo & Cooper, 2015).

3.3.4 Economic challenges

There is a global skills shortage of nearly 4 million cybersecurity experts, with this deficit set to grow amid an increase in demand for cyber professionals. At the same time, almost

90% of organizations experienced a breach in the last year, which they can partially attribute to a lack of cybersecurity skills. (Rashotte, 2024). Quader & Janeja (2021) highlight the importance of sufficient funding and investment in cybersecurity measures to strengthen IT infrastructure and defend against cyber threats. They argue that the greater the investment and effort organizations dedicate to cybersecurity, the more secure their network environments become. Conversely, insufficient investment leaves systems increasingly vulnerable to attacks. (Quader & Janeja, 2021)

According to Asen et al. (2019) it is not easy for companies to allocate appropriate amounts of budget to cybersecurity. Existing regulations do not offer specific guidance on cybersecurity budgeting. Cybersecurity requires partnerships between multiple departments and therefore the budgeting is also often distributed. Security rises for example procurement, technology and HR costs. (Asen et al., 2019).

There are multiple cases of cybersecurity incidents attributed to insufficient resources dedicated to cybersecurity. Although not an energy sector case, Equifax data breach that occurred in 2017 is a well-known case. The cause was a failure to patch a known vulnerability in their system due to resource and process deficiencies in IT security management (Novak & Vilsenau, 2019).

A core problem identified during REDISET work was a lack of cybersecurity resources. Subproblems included shortage of security specialists, insufficient resources to meet the digitalization requirements necessary to comply with evolving regulations (e.g., CO2 reduction), the complexity of cybersecurity work, and the prevalence of unknown or structured attacks. Safety is seen as expensive, and there is a lack of education, motivation, and research in the field. Other causes include the rapid pace of cybersecurity development and growing cyber threats that organizations struggle to keep up with, lack of knowledge, failure to apply updates and patches, and monopolistic control of data (e.g., U.S. dominance over platforms and data). Figure 17 demonstrates the different subproblems tied to lack of resources in regards of cyber security.

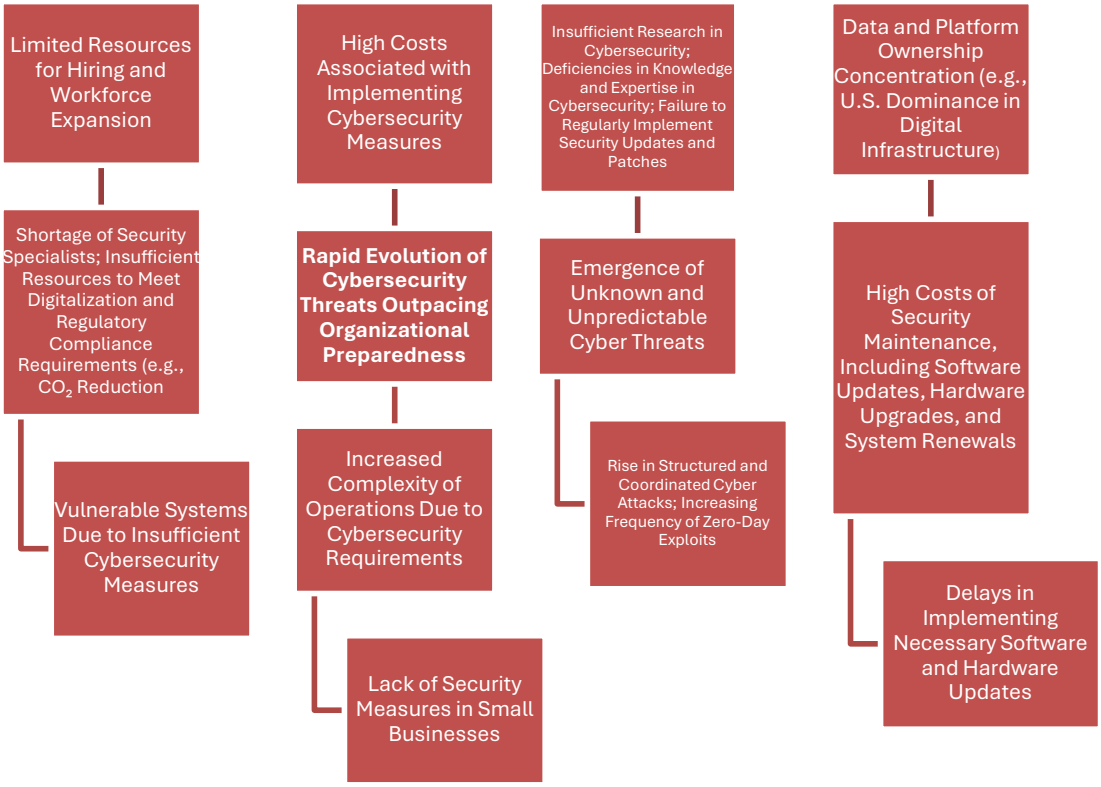

Figure 17. Lack of cybersecurity resources in terms of money and expertise.

The problems presented in Figure 17. lead to weakened systems vulnerable to attacks, leaving especially small businesses with inadequate security measures and contributing to an increase in zero-day attacks. Vulnerabilities are further increased by postponing software and hardware renewals.

3.3.4.1 Recommendations for addressing lack of cybersecurity resources

There is an increased need to prioritise cybersecurity in expenditures. Research indicates that cybersecurity breaches can affect labor productivity by disrupting operations or business processes including loss of data, revenue, time or damage to software (Hasan et al., 2021, Tetteh and Otioma 2024). Table 10. provides an overview of possible approaches to overcome resource-based challenges.

Table 10. Recommendations for addressing economic challenges.

Recommendation Area	Key Actions & Justification
Continuous improvement and research	- Encourage societal attitude changes to prioritize cybersecurity. - Advocate for increased cybersecurity budgets to support ongoing improvements. - Foster a culture where cybersecurity is seen as a strategic priority.
Assessing risk appetite and prioritizing accordingly	-Evaluate organizational risk appetite to determine which assets require protection. - Conduct asset inventories to identify critical data, systems, and processes that need prioritization. -Perform risk assessments to align cybersecurity investments with business priorities. - Utilize cybersecurity frameworks such as ISO27001 or NIST to guide budgeting and security strategies.

3.3.4.2 Continuous improvement and research

Societal attitude change is necessary for continuous improvement in cybersecurity.

Prioritizing cybersecurity within energy systems necessitates a transformation in societal attitudes. This transformation involves raising awareness about the significance of cybersecurity among the general public and key stakeholders. Effective strategies to achieve this include educational campaigns, public service announcements, and the integration of cybersecurity education into school curricula. The ultimate objective is to cultivate a culture where cybersecurity is perceived as vital for safeguarding both personal and national interests (Snider et al., 2021).

Shifting perspectives to recognize cybersecurity as a fundamental component of business and national security is crucial for ensuring adequate funding and resource allocation. Adequate funding facilitates the development and implementation of advanced security technologies, ensures continuous monitoring, and enables rapid responses to threats. Additionally, it supports training and development programs for cybersecurity professionals (Gordon et al., 2015). Continuous improvements in cybersecurity are only supported by increased budgets and if cybersecurity is not prioritized at an organizational or governmental level, budget allocations for security initiatives may remain insufficient. Thus, elevating cybersecurity to a strategic priority within organizational culture is essential. This involves embedding cybersecurity into the core strategy of organizations

and recognizing it as a critical component of overall risk management. Consequently, cybersecurity considerations should be integrated into decision-making processes at all organizational levels, from executive management to operational staff. (Hepfer and Powell, 2020).

3.3.4.3 Assessing risk appetite and prioritizing accordingly

It is essential to assess an organization's risk appetite to determine whether specific assets require protection or if other priorities should take precedence. Conducting an asset inventory allows businesses to identify which data, systems, or processes need special attention. By understanding which assets are most valuable, companies can implement security measures that align with their operational priorities. (Asen et al., 2019).

Organizations can further enhance their cybersecurity posture by performing a risk assessment and aligning their processes with established cybersecurity frameworks, such as ISO 27001 or NIST. This alignment helps determine necessary budgetary allocations and ensures that security investments support the organization's overall risk management strategy (Asen et al., 2019). Compliance with evolving regulatory recommendations is another critical factor in cybersecurity resilience. According to the NIS2 directive, organizations should evaluate and consider the resilience and quality of their products and services, as well as the cybersecurity risk management strategies integrated into them. Secure development procedures and cybersecurity policies of service providers and suppliers should also be assessed. Organizations must analyze risks associated with different levels of their supply chain, ensuring that relationships in supply chain management, procurement, and product lifecycle management align with security best practices. These measures help mitigate vulnerabilities and ensure that organizations meet the latest regulatory requirements (Directive (EU) 2022/2555).

4 CONCLUSIONS

The REDISET project aimed to provide a structured approach for managing socio-cyber-physical risks in the Nordic energy sector. The primary objective of the manual and the social manipulation checklist was to develop a comprehensive and accessible resource for policymakers, security officers, business developers, and other key stakeholders. By consolidating cybersecurity guidelines into a user-friendly format, the manual addresses one of the core challenges identified in the project—the fragmented nature of cybersecurity information and practices, which is often dispersed across multiple sources. This manual serves as a tool for improving compliance, operational efficiency, and decision-making in complex, safety-critical systems governed by strict regulatory frameworks, such as the EU Clean Energy Package. The checklist further enhances this resource by providing a self-assessment tool that allows stakeholders to measure their cybersecurity awareness and knowledge. This approach helps users to identify areas requiring further attention and enables them to engage with the manual in a targeted and efficient manner.

One of the most significant findings of the project is that cybersecurity culture varies significantly across organizations in the energy sector. Differences in skill levels, awareness, and training contribute to inconsistent cybersecurity practices and increasing vulnerabilities. Behavioral weaknesses remain a key issue, as human factors often represent the weakest link in mitigating cyber risks. Additionally, organizational shortcomings, such as insufficient safety procedures, poor communication between stakeholders, and the absence of a unified cybersecurity strategy, further weaken the energy sector's resilience. Another critical issue is the growing dependence on interconnected and interdependent systems, which introduces new vulnerabilities through unknown awareness, outdated protocols, lack of compatibility, and an expanded attack surface. Many organizations operate within trust-based cultures, where over-reliance on security regulations and reluctance to adopt new technologies contribute to unrecognized risks. Socio-cultural factors, such as resistance to complex cybersecurity rules and overwhelming task demands, further impede the adoption of security best practices. Additionally, employees often lack motivation to comply with stringent security protocols, highlighting the need for better engagement strategies. The rapid pace of technological advancements, particularly in AI-driven attacks, outpaces human understanding, creating new security challenges that many organizations struggle to address. The interconnected nature of energy systems means that failures can have cascading effects, emphasizing the importance of preparedness and resilience.

Given these challenges, a comprehensive cybersecurity strategy that integrates cultural, behavioral, technical, economic, and sociopolitical factors is essential. By focusing on education, awareness, cooperation, and strategic investments, alongside the adoption of

regulatory frameworks, the energy sector can significantly improve its cyber resilience and reduce the risks associated with evolving cyber threats.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. Computer Science & IT Research Journal, 5(1), 100-119.

Aichbauer, S., Buchhauser, M., Erben, A., Steinert, S., Tietze, D., & Wiking, E. (2022). *Responsible procurement: leading the way to a sustainable tomorrow* (p. 193). Springer Nature.

Alcaraz, C., & Lopez, J. (2014). A security analysis for SCADA protocols in smart grids. *Critical Infrastructure Protection*, 6, 67-74

Allcott, H., & Rogers, T. (2014). The short-run and long-run effects of behavioral interventions: Experimental evidence from energy conservation. *American Economic Review, 104*(10), 3003-3037

Althouse, J., et al. (2021). *Vulnerability Management in IoT Systems*. Journal of Cybersecurity Research, 8(3), 234-247.

Amin, S., Cárdenas, A. A., & Sastry, S. (2013). Safe and secure networked control systems under denial-of-service attacks. *Automatica*, 49(8), 1820-1831.

Ang, C. K. G., & Utomo, N. P. (2017, October). Cyber security in the energy world. In 2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT) (pp. 1-5). IEEE.)

Antunes, P., & Tate, M. (2022). Business process conceptualizations and the flexibility-support tradeoff. *Business Process Management Journal*, *28*(3), 856-875.

Asen, A., Bohmayr, W., Deutscher, S., González, M., & Mkrtchian, D. (2019). Are you spending enough on cybersecurity?. *Режим доступа: https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity (дата обращения 20.07. 2022*

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. *IT professional*, *13*(1), 12-15.

Badman A. (2023). *What is a phishing simulation? (Published online 9.8.2023).* IBM.com. Retrieved 3.2.2025 from https://www.ibm.com/think/topics/phishing-simulation

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A. Z., & Mahouachi, D. (2024). A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *Journal of Cybersecurity and Privacy*, *4*(4), 853-908.

Berg, P., Berlijn, S. M., Eltahawy, B., Hilber, P., Karimi, M., Klepper, K. B., ... & Xu, Q. (2024, May). Towards a Model for Assessing the Effects of Social-Cyber-Physical Threats on the Future Power Grid–Review and Workshop Results. In 2024 International Workshop on Artificial Intelligence and Machine Learning for Energy Transformation (AIE) (pp. 1-6). IEEE.

Boeding, M., Boswell, K., Hempel, M., Sharif, H., Lopez Jr, J., & Perumalla, K. (2022). Survey of cybersecurity governance, threats, and countermeasures for the power grid. *Energies*, *15*(22), 8692.

Boekelo, M., & Kloppenburg, S. (2023). Energy platforms and the future of energy citizenship. Energy Research & Social Science, 102, 103165.

Borenius, S., Gopalakrishnan, P., Bertling Tjernberg, L., & Kantola, R. (2022). Expert-guided security risk assessment of evolving power grids. *Energies*, *15*(9), 3237.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

Breitschopf, B., Grimm, A., Billerbeck, A., Wydra, S., & Köhler, J. (2023). Towards understanding interactions between socio-technical systems in sustainability transitions. Energy Research & Social Science, 106, 103323. https://doi.org/10.1016/j.erss.2023.103323

Burgett A. (2024). *Building Cyber Resilience with Scenario-Based Tabletop Exercises* (published online 23.10.2024). ArmorPoint.com. Retrieved 3.2.2025 from https://armorpoint.com/2024/10/23/building-cyber-resilience-with-scenario-based-tabletop-exercises/

Burrell, D. N. (2019). An exploration of the critical need for formal training in leadership for cybersecurity and technology management professionals. In *Human Performance Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1420-1432). IGI Global.

Bytyqi, B., et al. (2021). *A Review on TSO-DSO Data Exchange, CIM Extensions, and Interoperability Aspects*.

Cagnazzo, L., Taticchi, P., & Botarelli, M. (2020). Building competitive advantage through training and knowledge sharing. *Journal of Business Strategy*, 41(2), 43-50.

Campos, I., & Marín-González, E. (2020). People in transitions: Energy citizenship, prosumerism and social movements in Europe. Energy Research & Social Science, 69, 101718.

CARR, M. (2016). Public–private partnerships in national cyber-security strategies. *International affairs (London), 92*(1), 43-62. https://doi.org/10.1111/1468-2346.12504

Carreiro, A., et al. (2022). Hybrid models for TSO-DSO coordination in renewable integration. *Journal of Renewable Energy Systems, 45*(2), 134-150.

Carvalho, A. (2017). *Energy and Critical Infrastructure: Insights from Systemic Risks*

Carvallo, Andres, and John Cooper. *The advanced smart grid: Edge power driving sustainability*. Artech House, 2015.

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1).

CERRE (2016). *Technological Developments in Smart Energy Systems: Challenges for DSOs*. Centre on Regulation in Europe. Retrieved from https://cerre.eu

Chatchalermpun, S., & Daengsi, T. (2021, February). Improving cybersecurity awareness using phishing attack simulation. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1088, No. 1, p. 012015). IOP Publishing.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006.

Chernenko, E., Demidov, O., & Lukyanov, F. (2022). *Increasing international cooperation in cybersecurity and adapting cyber norms*. Council on Foreign Relations.

Child, M., Bogdanov, D., Aghahosseini, A., & Breyer, C. (2020). The role of energy prosumers in the transition of the Finnish energy system towards 100 % renewable energy by 2050. *Futures : the journal of policy, planning and futures studies, 124*, 102644. https://doi.org/10.1016/j.futures.2020.102644'

CISA (2024). *CISA Tabletop Exercise Packages: Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios.* America's Cyber Defence Agency. Retrieved 3.2.2025 from https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

Clausmeier, J. (2023). Digital Operational Resilience Act (DORA): Implications for financial entities. *Financial Cybersecurity Review*, 15(3), 89-102.

Conti, M., Dehghantanha, A., & Watson, S. (2020). Intrusion detection and response in the age of IoT: Advances and challenges. *Future Generation Computer Systems, 115*, 606–619. https://doi.org/10.1016/j.future.2019.11.001

Contreras, M., et al. (2023). Addressing legacy technologies in critical energy infrastructure. *Energy Infrastructure Quarterly, 8*(1), 67-78.

Cortade, T., & Poudou, J. (2022). Peer-to-peer energy platforms: Incentives for prosuming. *Energy Economics*, *109*, 105924. https://doi.org/10.1016/j.eneco.2022.105924

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), 698.

Cybersecurity and Infrastructure Security Agency (CISA). (2021). Lessons Learned from Colonial Pipeline Attack.

Dafalla, Y., Liu, B., Hahn, D. A., Wu, H., Ahmadi, R., & Bardas, A. G. (2020). Prosumer nanogrids: A cybersecurity assessment. *IEEE Access*, *8*, 131150-131164.

Darby, S. (2006). The effectiveness of feedback on energy consumption. *Environmental Change Institute, University of Oxford.*

Darby, S. (2010). Smart metering: What potential for householder engagement? *Building Research & Information*, *38*(5), 442–457. https://doi.org/10.1080/09613218.2010.492660

de Haan, J., et al. (2021). *Operational Manuals for Compliance in EU Energy Systems*. Energy Policy Journal, 58(4), 123-138.

Dhillon, H., & Hentea, M. (2005, March). Getting a cybersecurity program started on low budget. In *Proceedings of the 43rd annual Southeast regional conference-Volume 1* (pp. 294-300).

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, *24*(4), 1328.

Dinha, F. (2025). *Leadership In Cybersecurity Disruption: Turning Emerging Threats Into Competitive Opportunities (published online 9.4.2025).* Forbes Technology Council. Retrieved 15.4.2025 from https://www.forbes.com/councils/forbestechcouncil/2025/04/09/leadership-in-cybersecurity-disruption-turning-emerging-threats-into-competitive-opportunities/

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)

Dkaidek, Z., & Rashid, A. (2024). Bridging the Cybersecurity Skills Gap: Knowledge Framework Comparative Study. *IEEE Security & Privacy*, *22*(5), 88-95.

Oueslati, N. E., Mrabet, H., Jemai, A., & Alhomoud, A. (2019, December). Comparative study of the common cyber-physical attacks in industry 4.0. In *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)* (pp. 1-7). IEEE.

Efthymiou, C., & Kalogridis, G. (2010). Smart grid privacy via anonymization of smart metering data. *IEEE International Conference on Smart Grid Communications*, 238-243.

Ehsan, A., & Yang, Q. (2018). Optimal integration and planning of renewable distributed generation in the power distribution networks: A review of analytical techniques. *Applied Energy*, *210*, 44-59. https://doi.org/10.1016/j.apenergy.2017.10.106

Energy Authority, 2024: https://energiavirasto.fi/en/energy-authority

ENTOS-E (2021). *Cybersecurity Challenges in the Digitalized Grid*. European Network of Transmission System Operators for Electricity. Retrieved from https://www.entsoe.eu

Envall, F., Andersson, D., & Wangel, J. (2023). Gridlocked: Sociomaterial configurations of sustainable energy transitions in Swedish solar energy communities. Energy Research & Social Science, 102, 103200.

Ertz, M., Cao, X., & Barragán Maravilla, J. M. (2024). The Prosumer. *Encyclopedia (Basel, Switzerland), 4*(3), 1263-1278. https://doi.org/10.3390/encyclopedia4030082

Eurelectric. (2018). *Digitalizing Europe's energy system*. Retrieved from https://eurelectric.org

European Defence Agency (2024). https://eda.europa.eu/publications-and-data/factsheets/factsheet-eda-long-term-review-2024

European Defence Agency (2024). https://eda.europa.eu/webzine/issue11/in-the-field/sustaining-europe-s-armed-forces

EU (2024a). European Union. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

EU (2024b). European Union. https://www.europarl.europa.eu/factsheets/en/sheet/68/energy-policy-general-principles

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, *14*(4), 944-980. https://doi.org/10.1109/SURV.2011.101911.00087

Finnish Energy, 2024: https://energia.fi/en/energy-sector-in-finland/energy-market/

Fischer, C. (2008). Feedback on household electricity consumption: A tool for saving energy? *Energy Efficiency, 1*(1), 79-104.

Fischer, S. (2021). *Cybersecurity and energy infrastructure: A new frontier*. Wiley

Frederiks, E. R., et al. (2015). Household energy use: Applying behavioural economics to understand consumer decision-making and behaviour. *Renewable and Sustainable Energy Reviews, 41,* 1385-1394.

Frederiksen, T. K., Hesse, J., Lehmann, A., & Torres Moreno, R. (2019). Identity management: State of the art, challenges and perspectives. *IFIP International Summer School on Privacy and Identity Management*, 45-62.

Gellings, C. W. (2020). The smart grid: Enabling energy efficiency and demand response. *CRC Press*.

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*, 103199.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems*, *62*(4), 706–716. https://doi.org/10.1080/08874417.2021.1903367

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. Journal of

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, 62(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Georgiadou, A., Psarrou, A. M.., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*, 103199. https://doi.org/10.1016/j.cose.2023.103199

Gillingham, K., et al. (2018). The rebound effect and energy efficiency policy. *Review of Environmental Economics and Policy, 10*(1), 68-88.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3-17.

Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. *Energies*, *15*(19), 6984.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2010). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, *7*(4), 529-539. https://doi.org/10.1109/TII.2011.2166794

Hahn, A., & Govindarasu, M. (2011). Cybersecurity for SCADA systems in electric power systems: Protocols, policies, and services. *IEEE Security & Privacy*, *9*(6), 54-59. https://doi.org/10.1109/MSP.2011.144

Hale, A., et al. (2020). *The Role of Checklists in Energy Sector Safety and Training*. Safety Science, 125(6), 45-62.

Han, C., & Dongre, R. (2014). Q&A. What motivates cyber-attackers?. Technology innovation management review, 4(10).

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hatziargyriou, N. D., et al. (2006). Microgrids. *IEEE Power and Energy Magazine*, *5*(4), 78-94. https://doi.org/10.1109/MPAE.2006.1687811

Hepfer, M., & Powell, T. C. (2020). Make cybersecurity a strategic asset. *MIT Sloan Management Review*, *62*(1), 40-45.

Heras-Saizarbitoria, I., Dogui, K., & Boiral, O. (2013). Shedding light on ISO 14001 certification audits. *Journal of Cleaner Production*, *51*, 88-98.

Hess, D., & Sovacool, B. K. (2020). Sociotechnical matters: Reviewing and integrating science and technology studies with energy social science. *Energy Research & Social Science, 65,* 101462.

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. *Computers & Security*, *108*, 102357

Holm, H., Flores, W. R., & Ericsson, G. (2013, October). Cyber security for a smart grid-what about phishing?. In *IEEE PES ISGT Europe 2013* (pp. 1-5). IEEE.

https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

https://securityintelligence.com/news/proactive-cybersecurity-policy-smart-essential/?utm_source=chatgpt.com

Kungliga Tekniska Högskolan. REDISET Project website: https://www.kth.se/rediset

IBM 2024 https://www.ibm.com/topics/offensive-security

IEA (2020): *Power Systems in Transition*, IEA, Paris https://www.iea.org/reports/power-systems-in-transition, Licence: CC BY 4.0

IEC 62443-3-2. (2018). Security for industrial automation and control systems: Security risk assessment and system design.

Insurica. 2024. Retrieved from https://insurica.com/blog/colonial-pipeline-ransomware-attack/

Institutedata.com (2024). *Asking the Right Questions: Strategies for Effective Questioning Techniques in Cybersecurity (published online 20.6.2024).* Institute of Data. Retrieved 3.2.2025 from https://www.institutedata.com/us/blog/asking-the-right-questions-strategies-for-effective-questioning-techniques-in-cybersecurity/

International Energy Agency (2021). *Net zero by 2050: A roadmap for the global energy sector*. International Energy Agency. https://www.iea.org/reports/net-zero-by-2050

International Energy Agency (IEA). (2018). *World energy outlook 2018*. IEA.

Jamasb, T., & Pollitt, M. (2015). Electricity sector liberalisation and innovation: An analysis of the UK's reform. *Energy Journal, 26*(4), 29-54

Jararweh, Y., Otoum, S., & Al-Quraan, H. (2020). Software-defined micro-segmentation for security in smart grid networks. *Journal of Network and Computer Applications*, 170, 102789.

Javidi, M., Khalilzadeh, Z., & Malekzadeh, M. (2019). The impact of firewalls in preventing cyberattacks on enterprise networks. *International Journal of Computer Applications, 182*(38), 26–30. https://doi.org/10.5120/ijca2019918766

Jha, R. K. (2023). Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. *Recent Research Reviews Journal*, *2*(2), 215-241.

Kanna, I. V. (2023). Energy policies and standards. In *Elsevier eBooks* (pp. 9–20). https://doi.org/10.1016/b978-0-323-93940-9.00089-x

Karaman, M., & Aybar, C. (2016). Institutional cybersecurity from military perspective. International Journal of Information Security Science, 5(1), 1-7.

Kim, J., & Lee, S. (2020). A review of network segmentation for cybersecurity in IoT-based critical infrastructures. *IEEE Access*, 8, 125950-125964.

Kotilainen, K. (2019). Prosumer role in the sustainable energy system. In (W. Leal Filho, A. M. Azul, L. Brandli, P. G. Özuyar, & T. Wall, Eds.) Encyclopedia of the UN Sustainable Development Goals: Affortable and Clean Energy. Springer.

Kotilainen, K. (2020). *Perspectives on the prosumer role in the sustainable energy system: Dissertation*. [Dissertation, Tampere University]. University of Tampere. http://urn.fi/URN:ISBN:978-952-03-1576-4

Kotilainen, K., Mäkinen, S. J., & Järventausta, P. (2016, October). Understanding prosumers' intrinsic and extrinsic motivations to become active participants in smart grid innovation ecosystem. In *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE.

KPMG (2020). The state of corporate sustainability in global energy companies. *KPMG International Reports.*

Krasznay, C., & Hámornik, B. P. (2019). Human factors approach to cybersecurity teamwork – the military perspective. Advances in Military Technology, 14(2), 291-305. https://doi.org/10.3849/aimt.01296

Krause T., Ernst R., Klaer B., Hacker I., Henze M. (2021) Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*. 21 (18) :6225. https://doi.org/10.3390/s21186225

Krkoleva Mateska, A., Krstevski, P., & Borozan, S. (2021). Overview and improvement of procedures and practices of electricity transmission system operators in South East Europe to mitigate cybersecurity threats. *Systems, 9*(2), 39. https://doi.org/10.3390/systems9020039

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31*(12), 4488-4500.

Laczi, S.A., Póser, V. (2025). Mind the Gap: Introducing the "Generation Gap's Problem" in Cybersecurity. In: Kovács, T.A., Stadler, R.G., Daruka, N. (eds) The Impact of the Energy Dependency on Critical Infrastructure Protection. ICCECIP 2024. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-78544-3_37

Liang, X., & Zhao, Y. (2021). Blockchain for secure and compatible IoT systems: A survey. *Computers & Security, 101*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Lu, C., Guo, X., & Jin, L. (2020). Addressing interoperability issues in smart grid cybersecurity. *ACM Transactions on Cyber-Physical Systems, 4*(3), 17. https://doi.org/10.1145/3388442

Luiijf, E., & Klaver, M. (2015). *Cybersecurity in energy infrastructure: A cross-sectoral approach*. Springer

Macnish, K., & Van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in society*, *63*, 101382.

Marzband, M., et al. (2023). Cost optimization in DER integration: A case study. *Energy Policy, 133*(4), 23-45.

Mayorga, P. (2020). *TSO-DSO Cooperation and Dynamic Modeling for Secure Energy Systems*.

Macnish, K., & Van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in society*, 63, 101382.

McKinsey & Company. (2021). *The net-zero transition: What it would cost, what it could bring*. McKinsey & Company.

Milevskyi, S., Korchenko, O., & Yevseiev, S. (2023). Socio-cyber-physical systems' threats classifier. , 16–20. https://doi.org/10.21303/2585-6847.2023.003201

Miller, B., & Rowe, D. (2012, October). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology* (pp. 51-56).

Miller, C. A., et al. (2015). The social dimensions of energy transitions. *Science as Culture, 24*(2), 135-148.

Misuraca, G., & Viscusi, G. (2014, October). Digital governance in the public sector: challenging the policy-maker's innovation dilemma. In *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance* (pp. 146-154).

Mitropoulos, P., et al. (2020). *Patch Management Delays and Cybersecurity*. Security Management Quarterly, 14(1), 45-59.

Morstyn, T., Farrell, N., Darby, S. J., & McCulloch, M. D. (2018). Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants. *Nature Energy*, *3*(2), 94-101. https://doi.org/10.1038/s41560-017-0075-y

Mylrea, M., & Gourisetti, S. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale, and security. *Smart Grid Communications*, 2(4), 75-82.

Naqvi, B., Clarke, N., & Porras, J. (2021). Incorporating the human facet of security in developing systems and services. *Information & Computer Security*, *29*(1), 49-72.

National Cyber Security Centre Finland, 2024
https://www.kyberturvallisuuskeskus.fi/en

National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework.

Novak, A. N., & Vilceanu, M. O. (2019). "The internet is not pleased": twitter and the 2017 Equifax data breach. *The Communication Review*, 22(3), 196-221.

Oliveira, L., Rodolfo, M., & Barros, M. (2021). Overcoming legacy system challenges in IoT integration: A survey. *IEEE Transactions on Industrial Informatics, 17*(1), 91–102. https://doi.org/10.1109/TII.2020.2964437

Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. *Information & Computer Security*, *29*(3), 457-484.

Oueslati, N. E., Mrabet, H., Jemai, A., & Alhomoud, A. (2019, December). Comparative study of the common cyber-physical attacks in industry 4.0. In *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)* (pp. 1-7). IEEE.

Pagani, G., et al. (2019). Simulation frameworks for congestion management in distributed systems. *CIRED Conference Proceedings, 1158*, 1-10.

Papadaskalopoulos, D., et al. (2022). Regulatory challenges in energy system integration. *Energy Regulation Studies, 12*(3), 45-65.

Parra, D., Walker, G. S., & Gillott, M. (2017). Are batteries the optimum photovoltaic energy storage solution? Techno-economic comparison with other storage systems. *Renewable and Sustainable Energy Reviews*, *60*, 684-698.
https://doi.org/10.1016/j.rser.2016.01.004

Pintilie, E. (2021). Manipulation-A Characteristic of Human Behavior. New trends in Psychology, 3(2).

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, *Technology & Work*, 24(2), 371-390.

Ponemon Institute. (2021). Cost of a Data Breach Report.
https://www.ibm.com/reports/data-breach

Quader, F., & Janeja, V. P. (2021). Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. Journal of Cybersecurity and Privacy, 1(4), 638-659. https://doi.org/10.3390/jcp1040032).

Radha, V., & Reddy, D. H. (2012). A survey on single sign-on techniques. *Procedia Technology*, *4*, 134-139.

Radovanović, M., Filipović, S., & Pavlović, D. (2017). Energy security measurement–A sustainable approach. Renewable and Sustainable Energy Reviews, 68, 1020-1032

Rajivan, P., & Cooke, N. (2017). Impact of team collaboration on cybersecurity situational awareness. *Theory and Models for Cyber Situation Awareness*, 203-226.

Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity*, *6*(1).

Rashotte, R. (2024). Why closing the cyber skills gap requires a collaborative approach (published online 23.7.2024). Centre for Cybersecurity - World Economic Forum. Retrieved 3.2.2025 from https://www.weforum.org/stories/2024/07/why-closing-the-cyber-skills-gap-requires-a-collaborative-approach/

Rawal, B., & Peter, A. (2022). Quantum-safe cryptography and security. In Implementing and Leveraging Blockchain Programming (pp. 35-51). Singapore: Springer Nature Singapore.

Ridley, J. (2018). *Energy operations and safety: The role of engineering in critical systems*. Taylor & Francis

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, 23(8), 4060. https://doi.org/10.3390/s23084060

Sabahattini Mete, E. (2020). The Personality Traits in the Defense Industry: The Mediating Role of Organizational Citizenship Behavior. Sage Open, 10(4). https://doi.org/10.1177/2158244020982289

Salami, H., Okpara, K., Choochuay, C., & Kuaanan, T. (2024). Energy consumers barriers/motivations to becoming a prosumer. *Energy Efficiency*, *17*(8), 1-17.

Salmon, J. (2019). *Cybersecurity in industrial control systems: Protecting physical and digital assets*. Wiley

Schneider Electric. (2021). *Sustainability report 2021: Accelerating sustainable progress.* Schneider Electric.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., ... & Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, 166-182.

Shahzad, F., & Hussain, F. (2018). Emerging trends in IoT security and solutions: A systematic review. *Sensors*, 18(8), 2446.

Shell Sustainability Report. (2020). Available at: [https://reports.shell.com/sustainability-report/2020/]

Sivonen, M. H., & Kivimaa, P. (2024). Securitization of Energy Transitions in Estonia, Finland and Norway. *International Political Sociology*, *18*(3).

Smith, A., and Jones, B. (2022). *Emerging Trends in Cyberattacks*. Advanced Cyber Threats Journal, 16(2), 67-81.

Smith, D. C. (2021). Cybersecurity in the energy sector: are we really prepared?. Journal of Energy & Natural Resources Law, 39(3), 265-270.

Smith, R., et al. (2020). *Risk Management through Operational Guidelines in Energy Systems*. Journal of Energy Safety, 14(3), 78-89.

Snider, K. L., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1), tyab019.

Solansky, S. T., & Beck, T. (2021). Interorganizational information sharing: Collaboration during cybersecurity threats. *Public Administration Quarterly*, *45*(1), 105-122.

Soykan, Ustundag, E., & Bagriyanik, M. (2020). The effect of SMiShing attack on security of demand response programs. *Energies*, *13*(17), 4542.

Strielkowski, W., Kovaleva, O., & Efimtseva, T. (2022). Impacts of digital technologies for the provision of energy market services on the safety of residents and consumers. Sustainability, 14(5), 2934.

Storm, J. (2025). Intrusion Detection in Industrial Control Systems: Challenges in implementation and verification. University of Oslo.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417-432.

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), 2181.

TechAdvisory.org (2025). *A guide to implementing proactive cybersecurity measures.* Technology Advice for Small Businesses. Retrieved 3.2.2025 from https://www.techadvisory.org/2021/10/a-guide-to-implementing-proactive-cybersecurity-measures/

Tetteh, G. K., & Otioma, C. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics*, 1-22.

Thøgersen, J. (2017). Sustainable consumption: Basic concepts and issues. *Psychology and Marketing*, *34*(5), 462-468

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

Torres, C. I., & Crossler, R. E. (2024). Promoting security behaviors in remote work environments: Personal values shaping information security policy compliance. *Information Systems Research*.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573-586.

Tyson M. (2023). *7 cybersecurity mindsets that undermine practitioners and how to avoid them (published online 17.4.2023).* CSO.com. Retrieved 3.2.2025 from https://www.csoonline.com/article/575025/7-cybersecurity-mindsets-that-undermine-practitioners-and-how-to-avoid-them.html

Tvaronavičienė, M., Plėta, T., Della Casa, S., and Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, 2 (4), pp.802 - 813. https://doi.org/10.9770/ird.2020.2.4(6)

Vandezande, N. (2024). The NIS2 Directive: Enhancing cybersecurity across the EU. *Journal of Cybersecurity*, 10(2), 45-67.

Vishik, C., Sheldon, F., & Ott, D. (2013). Economic incentives for cybersecurity: Using economics to design technologies ready for deployment. In *ISSE 2013 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2013 Conference* (pp. 133-147). Springer Fachmedien Wiesbaden.

Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. *Springer International Publishing.*

Wang, P., & Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In *17th International Conference on Information Technology–New Generations (ITNG 2020)* (pp. 17-23). Springer International Publishing.

Wang, Z., Sun, L., & Zhu H. (2020) Defining Social Engineering in Cybersecurity. *IEEE Access*, Vol. 8, pp. 85094-85115, 2020, https://doi.org/10.1109/ACCESS.2020.2992807

Wangen, G. (2015). The role of malware in reported cyber espionage: a review of the impact and mechanism. *Information*, *6*(2), 183-211.

Winzer, C. (2012). Conceptualizing energy security. *Energy policy*, 46, 36-48.

Wu, Z., et al. (2020). The Evolution of Ransomware: Challenges and Solutions. *Journal of Cyber Threat Analysis*, 6(4), 88-103.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2018). A survey on smart grid communication infrastructures: Motivations, requirements, and challenges. *IEEE Communications Surveys & Tutorials*, 15(1), 5-20

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2018). A survey on smart grid communication infrastructures: Motivations, requirements, and challenges. *IEEE Communications Surveys & Tutorials, 15*(1), 5–20. https://doi.org/10.1109/SURV.2012.021312.00034

Yao, J., et al. (2023). Cybersecurity challenges in digital energy grids. *Energy Systems Cybersecurity, 14*(2), 89-105.

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future internet*, *11*(3), 63.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security*, *133*, 103412.

Zhang, C., Wu, J., Long, C., & Cheng, M. (2018). Review of existing peer-to-peer energy trading projects. *Energy Procedia*, *105*, 2563-2568.
https://doi.org/10.1016/j.egypro.2017.03.737

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.

Young, C. (2020). Incident Response Models (published online 12.8.2020). ISACA Journal. Retrieved 12.12.2024 from https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

Zugno, M., et al. (2022). *Dynamic Operational Manuals for the Modern Energy Sector*. Smart Grid Research Journal, 36(5), 112-130.

Zugno, M., et al. (2022). Real-time data exchange between TSOs and DSOs: Challenges and solutions. *Smart Grid Research Journal, 36*(5), 112-130.

Appendices

Appendix 1. AWARENESS

1. I am allowed to share my work passwords with colleagues.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. I am allowed to click on any links in emails from people I know.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

3. It's acceptable to use my social media passwords on my work accounts.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

4. I am allowed to open email attachments from unknown senders.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

5. I am allowed to download any files onto my work computer if they help me to do my job.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

6. I am allowed to enter my information on any website if it helps me do my job.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

7. I am allowed to send sensitive work files via a public Wi-Fi network.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

8. Sensitive print-outs can be disposed of in the same way as nonsensitive ones.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

9. If I find a USB stick in a public place, I shouldn't plug it into my work computer.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

10. I must not ignore poor security behaviour by my colleagues.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Q1: Total score 50 p.

Appendix 2. Answers and recommendations to questionnaire I AWARENESS.

1. I am allowed to share my work passwords with colleagues.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree
We suggest you check chapter Organizational cybersecurity and information security practices
2. I am allowed to click on any links in emails from people I know.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree
We suggest you check chapter Improving awareness

3. It's acceptable to use my social media passwords on my work accounts.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree

We suggest you check chapter Single Sign-On (SSO) and Identity Management and data encryption techniques

4. I am allowed to open email attachments from unknown senders.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree
We suggest you check chapter improving awareness
5. I am allowed to download any files onto my work computer if they help me to do my job.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree

We suggest you check chapter Secure Remote work policies

6. I am allowed to enter my information on any website if it helps me do my job.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree

We suggest you check chapter Individual cybersecurity behavior

7. I am allowed to send sensitive work files via a public Wi-Fi network.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree

We suggest you check chapter Developing and enforcing safety procedures and protocols
8. Sensitive print-outs can be disposed of in the same way as nonsensitive ones.
• Strongly Disagree
• Disagree
• Neutral
• Agree

• Strongly Agree
We suggest you check chapter Developing and enforcing safety procedures and protocols

9. If I find a USB stick in a public place, I shouldn't plug it into my work computer.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree
We suggest you check chapter Developing and enforcing safety procedures and protocols
10. I must not ignore poor security behaviour by my colleagues.
• Strongly Disagree
• Disagree
• Neutral
• Agree
• Strongly Agree

We suggest you check chapter : Poor organizational cybersecurity and information security practices

- Strongly Agree = 5 points
- Agree = 4 points
- Neutral = 3 points
- Disagree = 2 points
- Strongly Disagree = 1 point

Highest scores Q1 5x10= 50 p.

All in all if scored less than 70% (less than 35) point out also Inadequate assessment of own cyber capability (legacy thinking)

Table 11. Scoring for awareness quiz.

Level (0-5)	Description	Score Range (out of 50)
0 - Nothing	No knowledge, completely passive.	0 - 9
1 - Basic	Limited understanding and minimal protections.	10 - 19
2 - Compliance-Focused	Doing enough to meet rules and regulations.	20 - 29
3 - Proactive	Actively managing risks and improving security.	30 - 37
4 - Integrated	Actively managing risks and improving security.	38 - 44
5 - Leader	Leading the way and setting standards in security.	45 - 50

Appendix 3. Questionnaire II and III KNOWLEDGE.

1. Phishing refers to the practise of criminals sending unsuspecting users malicious emails. What does that make smishing?

- ☐ Sending users malicious social media messages
- ☐ Sending users malicious Skype messages
- ☐ Sending users malicious text (SMS) messages

2. And why has smishing become so dangerous in recent years?

- ☐ Smartphones make smishing easier to carry out
- ☐ More and more people are opening social media accounts
- ☐ More people are beginning to work remotely

3. What does VPN stand for?

- ☐ Virtual Private Network
- ☐ Valid Privacy Network
- ☐ Virtual Privacy Negotiator

3. When might you use a VPN?

- When tethering an internet connection from your mobile phone
- When connecting to the internet
- When connecting to the internet via public wifi

4. What's a man-in-the-middle attack?

- When cyber criminals target people through fake online dating profiles
- When cyber criminals intercept data sent electronically
- When cyber criminals stalk victims through social media sites

5. Why is your phone always asking you to install updates?

- So it can fix glitches
- So it can install updated anti-virus software
- So it can wipe confidential data

6. And which of the following is the best way to avoid email interception through public wifi?

- By using encryption software
- By using secure passwords
- By using a VPN

7. Which of the following best describes "Friday afternoon fraud"?

- The distribution of malware to coincide with weekends
- Phising people on Friday afternoons
- Insider attacks on employees' final days

Total score 70 p

Questionnaire III

1. Cookies are small information items (text files) stored in users' PCs and used widely by online service providers for several purposes, such as to capture user preferences (language, background colors, etc.), to identify the user when he/she uses a shopping list etc. By these means, cookies have indeed positive functions (e.g. they help avoiding the need to repeatedly have to identify yourself). However, cookies also raise some security and privacy concerns, for example:

- They could contain a virus which then infects my computer.
- The collection of data stored in my device.
- The collection of personal data as well as the risk that someone could impersonate me.

- I don't know.

2. One of your friends has recently been a victim of a social engineering attack since someone has stolen her username and password for accessing her work email. This name, "social engineering" looks quite strange to you as it puts together engineering with social issues. What does social engineering mean in a security context?

- Building systems that are easy to use for society.
- It is a form of social deception focused on information gathering, fraud, or system access.
- Someone uses social networks for stealing personal data.
- I don't know.

3. When you travel for work you often need to use open Wi-Fi networks, e.g. at train stations or coffee shops. However, you are aware that there might be dangers with such open networks. In order to protect your communication over these public networks you always:

- Use the private browsing function of your browser.
- Use a Virtual Private Network or VPN.
- Turn off your device's file sharing function.
- I don't know.

4. Passwords are strings of characters used to access online services (e.g. your email or social networks profile). However they also help to prevent other people from accessing your personal accounts. Unfortunately, because we use so many services, it is difficult to remember each password that we have. In this situation, what could be a good strategy?

- I save all my different passwords in a file: when I need one, I can easily retrieve it.
- I still prefer to use a different password each time.
- I use the same password for each service that I use.
- I don't know.

5. While opening the email, you got an interesting but suspicious message from a company. The message said that "you've won the lottery" and the company was asking you specific personal and banking details so that they could lodge a large sum of money in your bank account. These emails are a common type of cyber-attack that goes by the name of:

- Phishing
- spyware
- Spoofing
- I don't know.

6. Malware is software that has a malicious intent to harm users and their devices. A relevant protection in these cases is to have an antivirus software installed. However, even this is not sufficient as the antivirus needs to be constantly updated. What is your perspective about the need for updating the antivirus?

- I am updating of my antivirus should be performed only if I don't regularly patch my operating system.
- The antivirus update protects my computer from newly created malware.
- The antivirus updates ensure the correct performance of my computer.
- I don't know.

7. You have noticed that your computer is acting erratically and normal tasks (e.g., open a document/application), are taking a little bit longer to perform. So you called a friend of yours who is a computer technician and always helps you when your computer has problems. After a careful inspection he told you that your computer has been infected by a "Trojan Horse". You wonder what a "Trojan Horse" could be?

- It is a computer virus that frequently attack computers.
- It is a malicious software that allows other programs to control your computer by misleading users of its true intent.
- It is a malfunction of the software that makes it difficult to navigate the Internet.
- I don't know.

8. One day when looking at your e-mail inbox, you find you have received an email from a friend you have not heard from for at least one year. When you open the email the text says "Hi, please click here: http://shorturl.jhdsuyc.com, there is a surprise for you". What would you do in such scenario?

- You do nothing with the e-mail and, certainly, you don't click on the link.
- You click on the link, since you know the sender (friend) of the e-mail.
- You click on the link only if it looks somehow familiar to you.
- I don't know.

Total score 80 p (10 points for each correct answer)

Appendix 4. Answers and recommendations to questionnaire II and III KNOWLEDGE.

1. Phishing refers to the practise of criminals sending unsuspecting users malicious emails. What does that make smishing?

• Sending users malicious social media messages
• Sending users malicious Skype messages
• Sending users malicious text (SMS) messages CORRECT ANSWER (1 point)
--> We suggest you check chapter Individual cybersecurity behavior

2. And why has smishing become so dangerous in recent years?
• Smartphones make smishing easier to carry out CORRECT ANSWER (1 point)
• More and more people are opening social media accounts
• More people are beginning to work remotely
--> We suggest you check chapter Individual cybersecurity behavior

3. What does VPN stand for?
• Virtual Private Network CORRECT ANSWER (1 point)
• Valid Privacy Network
• Virtual Privacy Negotiator
--> We suggest you check chapter Challenges with the increased interconnection of systems
3. When might you use a VPN?
• When tethering an internet connection from your mobile phone
• When connecting to the internet
• When connecting to the internet via public wifi CORRECT ANSWER (1 point)
--> We suggest you check chapter Challenges with the increased interconnection of systems
4. What's a man-in-the-middle attack?
• When cyber criminals target people through fake online dating profiles
• When cyber criminals intercept data sent electronically CORRECT ANSWER (1 point)
• When cyber criminals stalk victims through social media sites
--> We suggest you check chapter Individual cybersecurity behavior

5. Why is your phone always asking you to install updates?
• So it can fix glitches
• So it can install updated anti-virus software CORRECT ANSWER (1 point)
• So it can wipe confidential data
--> We suggest you check chapter Challenges with the increased interconnection of systems

6. And which of the following is the best way to avoid email interception through public wifi?
• By using encryption software
• By using secure passwords
• By using a VPN CORRECT ANSWER (1 point)
--> We suggest you check chapter Challenges with the increased interconnection of systems

7. Which of the following best describes "Friday afternoon fraud"?
• The distribution of malware to coincide with weekends
• Phising people on Friday afternoons
• Insider attacks on employees' final days CORRECT ANSWER (1 point)
--> We suggest you check chapter Developing and enforcing safety procedures and protocols
total score 70 (10 points per 1 point)

Questionnaire III

1. Cookies are small information items (text files) stored in users' PCs and used widely by online service providers for several purposes, such as to capture user preferences (language, background colors, etc.), to identify the user when he/she uses a shopping list etc. By these means, cookies have indeed positive functions (e.g. they help avoiding the need to repeatedly have to identify yourself). However, cookies also raise some security and privacy concerns, for example:

• They could contain a virus which then infects my computer.
• The collection of data stored in my device. CORRECT ANSWER (1 point)
• The collection of personal data as well as the risk that someone could impersonate me.

- I don't know.

--> We suggest you check chapter Challenges with the increased interconnection of systems

2. One of your friends has recently been a victim of a social engineering attack since someone has stolen her username and password for accessing her work email. This name, "social engineering" looks quite strange to you as it puts together engineering with social issues. What does social engineering mean in a security context?

• Building systems that are easy to use for society.
• It is a form of social deception focused on information gathering, fraud, or system access. CORRECT ANSWER (1 point)
• Someone uses social networks for stealing personal data.
I don't know.

➔ We suggest you check chapter Individual cybersecurity behavior

3. When you travel for work you often need to use open Wi-Fi networks, e.g. at train stations or coffee shops. However, you are aware that there might be dangers with such open networks. In order to protect your communication over these public networks you always:

- • Use the private browsing function of your browser.
- • Use a Virtual Private Network or VPN. CORRECT ANSWER (1 point)
- • Turn off your device's file sharing function.
- I don't know.

  ☐ We suggest you check chapter Challenges with the increased interconnection of systems

4. Passwords are strings of characters used to access online services (e.g. your email or social networks profile). However they also help to prevent other people from accessing your personal accounts. Unfortunately, because we use so many services, it is difficult to remember each password that we have. In this situation, what could be a good strategy?

- • I save all my different passwords in a file: when I need one, I can easily retrieve it.
- • I still prefer to use a different password each time. CORRECT ANSWER (1 point)
- • I use the same password for each service that I use.
- I don't know.

☐ We suggest you check organizational cybersecurity and information security practices (especially **Secure Remote work policies**)

5. While opening the email, you got an interesting but suspicious message from a company. The message said that "you've won the lottery" and the company was asking you specific personal and banking details so that they could lodge a large sum of money in your bank account. These emails are a common type of cyber-attack that goes by the name of:

- • Phishing CORRECT ANSWER (1 point)
- • Spyware
- • Spoofing
- I don't know.
- ➔ We suggest you check ~~o~~rganizational cybersecurity and information security practices

6. Malware is software that has a malicious intent to harm users and their devices. A relevant protection in these cases is to have an antivirus software installed. However, even this is not sufficient as the antivirus needs to be constantly updated. What is your perspective about the need for updating the antivirus?

- • I am updating of my antivirus should be performed only if I don't regularly patch my operating system.
- • The antivirus update protects my computer from newly created malware. CORRECT ANSWER (1 point)
- • The antivirus updates ensure the correct performance of my computer.
- I don't know.
- ➔ We suggest you check Technological development is faster than human understanding of it

7. You have noticed that your computer is acting erratically and normal tasks (e.g., open a document/application), are taking a little bit longer to perform. So you called a friend of yours who is a computer technician and always helps you when your computer has problems. After a careful inspection he told you that your computer has been infected by a "Trojan Horse". You wonder what a "Trojan Horse" could be?
It is a computer virus that frequently attack computers.

- • It is a malicious software that allows other programs to control your computer by misleading users of its true intent. CORRECT ANSWER (1 point)
- • It is a malfunction of the software that makes it difficult to navigate the Internet.
- I don't know.
- ☐ We suggest you check Technological development is faster than human understanding of it

8. One day when looking at your e-mail inbox, you find you have received an email from a friend you have not heard from for at least one year. When you open the email the text says "Hi, please click here: http://shorturl.jhdsuyc.com, there is a surprise for you". What would you do in such scenario?

- You do nothing with the e-mail and, certainly, you don't click on the link. CORRECT ANSWER (1 point)
- You click on the link, since you know the sender (friend) of the e-mail.
- You click on the link only if it looks somehow familiar to you.
- I don't know.
- ➔ We suggest you check

total score 80 (10 points per 1 point)

Table 12. Quiz scoring for knowledge quiz.

Level (0-5)	Description	Score Range (out of 150)
0 - Nothing	No knowledge, completely passive.	0 - 29
1 - Basic	Limited understanding and minimal protections.	30 - 59
2 - Compliance-Focused	Doing enough to meet rules and regulations.	60 - 89
3 - Proactive	Actively managing risks and improving security.	90 - 109
4 - Integrated	Security is a key part of daily operations.	110 - 129
5 - Leader	Leading the way and setting standards in security.	130 - 150