‘It’s Confusing, Insecure, and Messy’ – Mapping the Gaps Between Stakeholders’ Cybersecurity Mental Models in the Danish Defence Sector

Judith Kankam-Boateng
Mathematics and Computer Science
University of Southern Denmark
Odense, Denmark
jukan@imada.sdu.dk

Marco Peressotti
Mathematics and Computer Science
University of Southern Denmark
Odense, Denmark
peressotti@imada.sdu.dk

Jan Stentoft
Department of Entrepreneurship and Relationship Management
University of Southern Denmark
Kolding, Denmark
stentoft@sam.sdu.dk

Kent Adsbøll Wickstrøm
Department of Entrepreneurship and Relationship Management
University of Southern Denmark
Kolding, Denmark
kwj@sam.sdu.dk

Vincent Charles Keating
Centre for War Studies
University of Southern Denmark
Odense, Denmark
keating@sam.sdu.dk

Louise Alison Tumchewics
Centre for War Studies
University of Southern Denmark
Odense, Denmark
ltu@sam.sdu.dk

Olivier Schmitt
Defence Academy
Royal Danish Defence College
Copenhagen, Denmark
olsc@fak.dk

Amelie Theussen
Defense Academy
Royal Danish Defence College
Copenhagen, Denmark
amth@fak.dk

Peter Mayer
Department of Mathematics and Computer Science
University of Southern Denmark
Odense, Denmark
Institute of Applied Informatics and Formal Description Methods
Karlsruhe Institute of Technology
Karlsruhe, Germany
mayer@imada.sdu.dk

Figure 1: Research Design approach. Structure of the qualitative study conducted in 2024 (N = 45). Participants were categorised into three groups: policy makers (Phase 1, one-day workshop in Month 1, n=6), policy promoters (Phase 2, one-day workshop in Month 2, n=11), and policy implementers(Phase 3, four workshops conducted within 1 Month, n=12 companies, 28 participants).

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791032

Abstract

Small and medium-sized enterprises (SMEs) are facing growing cybersecurity threats amidst limited resources and regulatory complexity. This complexity stems from diverse stakeholders in the regulatory process, including policymakers, industry associations, and companies that must implement the regulations. Misalignments between these different stakeholders can further compound the

complexity. Against this backdrop, we investigate the cybersecurity mental models held by three stakeholder groups in Denmark's defence sector and how these mental models might influence regulatory processes. Using a qualitative approach combining focus groups with 6 policymakers, 11 policy promoters (industry associations), and 12 policy implementers (SMEs), we reveal key misalignments in perceptions of risk, threats, cyber readiness, and policy interpretation. Our findings further show that SMEs often treat cybersecurity as a compliance task, while policymakers assume strategic readiness. Based on our results, we suggest recommendations for aligning governance frameworks with organisational realities.

CCS Concepts

• **Security and privacy → Social aspects of security and privacy**; *Economics of security and privacy*; • **Human-centered computing → Empirical studies in HCI**; • **Applied computing →** Supply chain management.

Keywords

Focus Group, Mental Models, Danish SMEs, Defence sector, Supply Chain, Policy Alignment

ACM Reference Format:

Judith Kankam-Boateng, Marco Peressotti, Jan Stentoft, Kent Adsbøll Wickstrøm, Vincent Charles Keating, Louise Alison Tumchewics, Olivier Schmitt, Amelie Theussen, and Peter Mayer. 2026. 'It's Confusing, Insecure, and Messy' – Mapping the Gaps Between Stakeholders' Cybersecurity Mental Models in the Danish Defence Sector. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 26 pages. https://doi.org/10.1145/3772318.3791032

1 Introduction

Cybersecurity poses significant challenges for organisations of all sizes [70, 93, 111]. Digital transformation introduces new vulnerabilities, while increasing global interconnectedness renders supply chain attacks, including cybersecurity and geopolitical issues, more prevalent and disruptive [3, 38, 79, 107, 130]. Recent supply chain breaches have created global impacts. The SolarWinds breach (2020) [32, 98], the Kaseya attack (2021) [32], the XZ open-source project compromise (2024) [32, 112] and the OpenJS Foundation social engineering takeover attempts (2024) [38, 47] all substantiate how supply chain vulnerabilities can cascade across interconnected systems. Although extensive research exists on cybersecurity, most studies focus on large corporations, with less attention to SMEs [51]. However, prior research shows that SMEs are frequently exploited as entry points by cybercriminals targeting larger organisations [32, 95] or by cybercriminals targeting SMEs [6, 32]. Furthermore, SMEs face distinct challenges as essential supply chain components that typically operate with limited resources [6, 7, 37].

In Denmark, SMEs constitute approximately 99% of businesses [19, 114], and many play vital roles in the defence supply chain. Nonetheless, their cybersecurity practices often lack consistency [33, 34, 40]. Recent findings indicate that 40% of Danish SMEs do not fully meet their security risk profiles, with outdated security documentation revealing significant gaps between their cybersecurity awareness and actual implementation [27]. Denmark faces a "very high cyber threat" as digitisation has elevated cyber threats from minor issues to matters of national security [20, 55]. At the time of Jensen's study [55], the defence sector was tasked with coordinating Denmark's cyber strategy across 13 ministries. Nevertheless, individual sectors have "excellent insight into their own operations, but limited outlook of cross-sector interdependencies" [55], creating a governance gap that weakens national resilience. With significant critical infrastructure held by private entities, the state cannot outsource responsibility for security even when operational tasks are delegated [28]. This requires the defence sector to develop effective mechanisms for coordinating resilience across public and private boundaries.

The Danish defence ecosystem presents a unique socio-technical environment characterised by high institutional trust, tight interdependent supplier networks, and a perception of "being too small to be targeted." This high-trust context provides an informative contrast to extensively studied low-trust environments such as the United States [77, 78]. Moreover, the defence sector calls for particular research attention due to its dual role as both a beneficiary of geopolitical tensions in Northern Europe and a potential source of systemic risk transmission to interconnected industries. The sector faces structural vulnerabilities [45], including rising operational costs, regulatory sanctions exposure, and supply-chain fragilities that become more pronounced in adverse situations [46]. It is essential for policymakers, companies, and investors to understand how the defence sector responds to various risk scenarios, as it often acts as an early indicator of the broader propagation of geopolitical risks to energy, cybersecurity, and critical infrastructure [60]. Given Danish defence companies' increasing operational and technological convergence with cybersecurity [2] and their reliance on global supply chains, exploring stakeholders' mental models remains under-explored.

Mental models—individuals' internal representations of how systems work—influence cybersecurity behaviours and decision-making [18, 126]. Early qualitative work established the importance of users' mental representations, though it primarily provided descriptive insights [4, 18]. Subsequent experimental studies examined whether familiar metaphors from medicine, crime, and physical security could enhance security reasoning, yet these interventions showed limited effectiveness [14]. Building on this foundation, Wash introduced a systematic taxonomy categorising eight "folk models" that shape users' threat perceptions [126]. Recent research has revealed persistent misalignments between expert and non-expert mental models [16, 54, 88, 127, 128], suggesting ongoing discrepancies in risk perceptions and security practices that may explain gaps between security advice and actual user behaviours. Additional studies have explored mental models in specific contexts, including risk communication, security warnings [4, 15, 101, 102], and organisational security attitudes [96].

Research on mental models in organisational cybersecurity, particularly in multi-stakeholder environments like defence supply chains, is limited. A key gap is the understanding of potential misalignments among the main stakeholders influencing SME cybersecurity: policymakers, who set national strategy; policy promoters, such as industry associations that provide guidance; and policy implementers, who apply these policies within SMEs.

To explore this gap, we conducted a qualitative study on the mental models of these three groups in Denmark's defence supply chain. Through focus group discussions, we explored how these stakeholders view their responsibilities, threats, risks, and challenges related to cybersecurity and supply chains. We address the following research questions:

RQ1: How do policymakers (PM), policy promoters (PP), and policy implementers (PI) perceive Denmark's current cybersecurity posture regarding national standards, strategies, and initiatives?

RQ2: How do these stakeholders evaluate Denmark's cybersecurity preparedness relative to international benchmarks?

RQ3: What are the views of these stakeholders on the policy implementers (PI) readiness for emerging global cybersecurity threats?

Our findings reveal key disconnects: policymakers prioritise regulatory strategies and national defence, while SMEs focus on survival and customer relationships. Policy promoters struggle to bridge the gap between high-level concepts and practical realities, leading to inconsistent adoption and misunderstandings of responsibilities. Notably, even effective policies may falter when stakeholders lack a shared understanding of cybersecurity in their specific contexts. While prior research on mental models emphasised usability and individual user behaviours, we show that eliciting mental models can uncover misalignments between governance and company levels that influence cybersecurity readiness. This can also guide the development of future cybersecurity awareness and training programs. This paper contributes:

C1: We provide a novel empirical mapping of cybersecurity practices and perceptions among Danish SMEs in the defence sector. We are the first to compare mental models across stakeholders (PM, PP, & PI) to identify themes and gaps that hinder effective policy translation.

C2: We outline issues that user-centred cybersecurity inventions, such as interactive awareness measures, need to consider which stakeholder group they are targeted at. To that end, we suggest targeted cybersecurity awareness measures to help address policy communication and mental model gaps.

We help PIs in identifying the capabilities needed to mitigate vulnerabilities and enhance company awareness and preparedness. Our study represents the first effort to map the mental models of three distinct stakeholders in cybersecurity. Our contribution is not merely identifying these issues but also highlighting how stakeholders' mental models differ in high-trust cultural contexts—a factor largely overlooked in existing literature focused on low-trust environments like the USA [77, 78]. In a similar vein, our contributions align with the HCI community's interest in how people collaborate, coordinate, and build shared meaning in complex security environments. Our work informs how interventions that shape users' interactions with cybersecurity technologies should be designed.

2 BACKGROUND

In this section, we situate our study with these four intersecting themes: (1) cybersecurity challenges in SMEs, (2) supply chain and supply chain resilience, (3) gaps in stakeholder awareness and governance, and (4) the role of mental models in cybersecurity.

2.1 Cybersecurity Challenges in SMEs

There are different definitions of SMEs across countries. For example UK [25], USA [12, 81], Canada [41]) and organizations (e.g., the OECD [86, 87] and WTO [131–133]). We will apply the EU's definition of SMEs (i.e., <250 staff) for this study. For the detailed definitions, refer to Appendix A.1. Regardless of their definitions, SMEs are essential contributors to national economic development and growth. SMEs are recognised as key drivers of both national and regional development in many countries. Research consistently emphasises their importance in achieving crucial socio-economic goals, such as job creation, increased output, export promotion, and support for entrepreneurship. [8, 39, 58, 131, 133].

In Denmark, the country where we conducted our research, SMEs account for 99% of businesses [19, 30, 114], contribute 60.8% value added and 64.1% of employment [30]. Danish SMEs are also described as the nation's "growth locomotive" by Dansk Industri [23]. Despite their economic significance, SMEs face growing cybersecurity threats [3, 111, 130]. Also, studies indicate that SMEs often underestimate their value to cybercriminals [105, 120]. They possess substantial data that makes them attractive, vulnerable targets. Some of their key challenges include limited resources, a lack of specialised expertise, and awareness gaps, which often result in cybersecurity being managed by non-specialists [6, 7, 37, 66, 89, 118]. Cybersecurity breaches cause multidimensional harm to SMEs, including financial losses, reputational damage, operational disruption, and psychological impacts [43, 80, 92]. Attackers often exploit SMEs as entry points to larger organisations and supply chains [37].

Danish SMEs are plagued by inconsistent cybersecurity practices. 40% operate below adequate security levels [27]. Only 76% adhere to basic practices such as updates and backups [27]. Also, 74% of management express involvement in cybersecurity initiatives and 70% are willing to enhance security practices [33]. The behavioural and organisational aspects of SME cybersecurity present additional complexity. Stentoft et al. conducted a survey of 248 individuals from Danish SMEs and found that there is still a gap between awareness of cybersecurity and action to address it [116]. Highlighting the ongoing research issue regarding the gap between cybersecurity awareness and its practical implementation, it indicates that raising awareness alone is not enough to drive behavioural change [6]. Firewalls, encryption, and detection tools are still very important, but they don't always solve the behavioural, organisational, and interpretive problems that come with implementing cybersecurity.

2.2 Supply Chain and Supply Chain Resilience

Recent crises like COVID-19 [115] and the war in Ukraine [10, 107] have exposed how fragile global supply chains can be, with disruptions spreading quickly across sectors [21, 35, 52]. Digitalisation and technologies such as IoT and cloud computing have increased these risks by expanding the threat surface and blurring IT and operational boundaries [67]. As a result, cybersecurity is now central to supply chain resilience. While prior work has advanced our understanding of cyber supply chain risk and resilience, several gaps remain unresolved.

First, much of the literature is fragmented across domains, with technical studies focusing on detection and prevention [5, 91] and organisational work emphasising governance and policy [13, 123].

Few frameworks adequately integrate these perspectives to account for the sociotechnical nature of supply chain resilience, where technologies, people, and institutions interact in complex ways.

Second, despite calls for improved visibility and coordination [22, 44], empirical evidence on how firms, particularly SMEs, achieve this in practice remains limited. SMEs are both vital to supply chains and disproportionately vulnerable due to resource and awareness constraints [6, 7]. Yet, most resilience models assume the capacity of large organizations.

Third, emerging paradigms such as Zero Trust architectures [134] and blockchain-enabled traceability [68] show promise and have been extensively explored in the supply chain. Yet, research to date has largely focused on technical feasibility rather than the organisational, regulatory, and multi-stakeholder conditions necessary for successful adoption. Similarly, the sustainability perspective integrating resilience with social and environmental responsibility, remains at the margins [106].

Beyond technical defences, research stresses the human and organisational dimensions of resilience. Bada and Nurse [6] highlight persistent awareness and training gaps among SMEs, while Manganaro [71] frames supply chain security as a people problem, with everyday employees as the first line of defence. Simon and Omar [113] show that attackers exploit uncoordinated investments across firms, underscoring the importance of collective governance and alignment. This insight echoes Melnyk et al. [75, 76], who argue that cybersecurity should be reframed as a supply chain issue rather than a siloed IT function. There is limited attention to the human dimensions of resilience: how perceptions, misaligned incentives, and cultural practices shape investments and behaviours across networks [71, 113]. This misalignment leads to underinvestment and fragmented defences, even as attackers exploit these systemic weaknesses.

2.3 Multi-stakeholders Gaps in Cybersecurity

Cybersecurity involves multiple stakeholder groups, each with distinct responsibilities and perspectives. This multi-stakeholder nature creates complex coordination challenges that extend far beyond technical implementation to encompass organisational, policy, and cognitive dimensions. The effectiveness of cybersecurity governance depends not only on individual stakeholder capabilities but critically on the alignment and coordination among diverse actors within the broader ecosystem. Research shows that strategic cybersecurity policies developed at national or organizational levels often fail to translate effectively into operational practices at implementation levels [57]. This translation gap reflects fundamental differences in how various stakeholders conceptualize cybersecurity risks, interpret their responsibilities, and prioritize appropriate responses [103]. policymakers may emphasize national resilience and geopolitical positioning, while SMEs focus primarily on business continuity and regulatory compliance [103]. These different framings can lead to policies that appear comprehensive at the strategic level but prove unworkable in operational contexts [90]. Despite growing recognition of these multi-stakeholder coordination challenges and their importance for cybersecurity outcomes, empirical research comparing how different stakeholder groups actually understand their roles, responsibilities, and relationships remains surprisingly limited, particularly in critical infrastructure sectors where public-private coordination is both essential and complex.

In this paper, we use the term "stakeholders" to refer to the three different participant groups central to our research: policymakers (PM), policy promoters (PP) and policy implementers (PI). Our focus is on the extent to which these groups' mental models of cybersecurity align or misalign. **policymakers (PMs** (comprising top officials from national security and the Ministry of Foreign Affairs) align cybersecurity initiatives with organisational objectives. They must balance considerations such as long-term risk, regulatory compliance, and organisational reputation. **Policy Promoters (PPs)** (industry-level experts, including officials from business associations from the defence sector) contribute specialized expertise and typically rely on established frameworks, standards, and assessments, including the NIST Cybersecurity Framework (NIST, 2018) [83] and NIS2 [31], to guide structured approaches to risk assessment and mitigation. **Policy Implementers (PIs)** in our research are SMEs who put these policies into practice.

2.4 Mental Models in Cybersecurity

Security failures often stem from misalignments between system design, expert recommendations, and user understandings. Cognitive science explains these through the concept of mental models: an internal representation people construct to reason about complex domains [56]. Camp [17, 18] first applied this framework to computer security, showing that users rely on familiar analogies (crime, medical infections, markets, and physical security) to understand cybersecurity, creating gaps between expert intentions and user perceptions.

Empirical research confirmed these misalignments. Asgharpour and Camp [4] demonstrated that experts and non-experts categorise threats differently. Wash [126] identified eight "folk models" of malware and hackers that, while often inaccurate, are internally coherent and shape user decisions. Bravo-Lillo et al. [15] found novices misunderstand browser warnings while experts dismiss them. Stobert et al. [117] observed clinicians bypassing security for patient care, while Wolf et al. [128] documented misconceptions in biometric authentication. Studies by Rader and Wash [100] and Das et al. [24] showed that stories and social influence transmit security lessons more effectively than formal training. Research on security advice reveals persistent gaps between expert and non-expert practices. Ion et al. [54] found experts favour updates, two-factor authentication, and password managers, while non-experts rely on antivirus and frequent password changes. Ortloff et al.'s [88] ten-year follow-up showed progress in 2FA adoption but continued resistance to password managers. Zou et al. [135] revealed that inconvenient practices are often abandoned, while Sasse [109] noted that coercive approaches rarely succeed.

Users act rationally within their mental models and contexts. While some gaps have narrowed (e.g., 2FA adoption), others persist (e.g., password manager uptake). However, to the best of our knowledge, no studies have examined differences in mental models among stakeholder types in areas such as national security, regulatory ecosystems [37], sector associations, and companies. SMEs must balance compliance with operational realities, yet little

is known about how policymakers, policy promoters, and policy implementers conceptualise terms such as "zero trust" and "resilience" [32, 38, 83, 134]. Without aligned communication, policy directives may fail if implementers view cybersecurity as external or optional rather than strategic and necessary.

This study fills that gap by examining how three types of groups: (1) policymakers, (2) policy promoters (such as industry associations), and (3) policy implementers (like SMEs) perceive cybersecurity. There has been considerable study on governance, compliance, and technological readiness; however, there is a lack of research on comparing and mapping cybersecurity mental models across different levels of stakeholders in security-sensitive areas such as the defence sector and supply chains. While understanding individual mental models provides crucial insights, addressing systemic cybersecurity challenges requires examining how these models align or diverge across different stakeholder groups. In complex policy environments where multiple organisations must coordinate their security efforts, misaligned mental models can undermine even technically sound security frameworks.

3 METHODOLOGY

We conducted a qualitative study to elicit the mental models of policymakers (PMs), Policy promoters (PPs), and Policy Implementors (PIs), specifically SMEs.

3.1 Study Design and Procedure by Levels

For our study, we conducted focus group discussions [64, 65] with participants from each of the three levels, i.e., PMs, PPs, and PIs, as workshops in 2024. For each focus group discussion, we had dedicated semi-structured guides (the full guides are available in Appendix A.2, Appendix A.3, and Appendix A.4). All sessions were conducted in English and facilitated by the same researcher to ensure consistency. At the beginning of each session, participants filled out an informed consent form (see Appendix A.5). Then the actual focus group discussion began and was recorded, and the recordings were stored in encrypted form. In each discussion we asked participants to share their perceptions on the following themes: (1) understanding the current cybersecurity posture and practices, (2) threats, vulnerabilities, and preparedness, (3) training, awareness, and communications, (4) challenges, approaches, and risk assessments, (5) resources, regulations, initiatives, and feedback, and (6) supply chain risks. Sessions lasted between 75 and 125 minutes (detailed in table 1).

3.2 Participants Demographics and Sampling

In total, 45 participants were recruited: 6 policymakers, 11 policy promoters, and 28 representatives from 12 SMEs (3-4 representatives per company). See table 2 for an overview of the participant demographics. In the following, we briefly outline the recruitment procedure and the participant sample for each level.

Policymakers Level. We recruited 6 participants (4 men, 2 women) as PMs, who were senior officials from national security institutions and the Ministry of Foreign Affairs. PMs were recruited through the research team's professional networks. No financial incentives were provided.

Policy Promoters Level. We recruited 11 participants (9 men, 2 women) as PPs, who were industry association experts representing the defence sector. PPs were also recruited through the research team's professional networks. No financial incentives were provided.

Policy Implementers Level. PIs were recruited from a public company register of Danish SMEs. Companies were first screened to identify those meeting our criteria: (1) small-to-medium enterprise status, (2) operations in the defence sector and (3) with SME participants proficient in English. Qualifying companies were then contacted via email with follow-up calls to recruit participants. The PI group consisted of 23 men and 5 women, representing 12 SMEs, selected from across all Danish regions. It was optional to speak Danish, though no company chose to use it.

3.3 Positionality

Our team comprises researchers specialising in cybersecurity, supply chains, and geopolitics. Two of the researchers are actively engaged with Danish SMEs in supply chain-related activities. Three researchers in the team are actively engaged in geopolitics-related activities with government entities. Two researchers are actively engaged in cybersecurity-related activities with national stakeholders. The team possesses considerable proficiency in qualitative analysis. We acknowledge that our origins influenced the study design. We upheld reflexivity throughout the process [36]. Our objective was not to engage in detached observation but to achieve an inclusive, contextual understanding of stakeholder experiences in cybersecurity governance [99].

3.4 Data Analysis

All discussions were audio-recorded and later transcribed. Applying a mixture of inductive coding [121], one researcher open-coded the transcript to identify emerging themes. PI participants were also given response sheets during the discussions to jot down and summarise their thoughts and responses to the questions we asked. We collected these response sheets after the discussions and included them alongside the transcripts in the analysis.

The coding process was performed in three phases. Firstly, we inductively coded all transcripts using in vivo coding, using the participants' own words as codes. This led to 592 initial open codes. Then, we used axial coding to explore relationships between codes, resulting in a reorganisation of the codes into 23 thematic categories. Finally, we developed three overarching themes for the categories [108].

To ensure analytical rigour and transparency in our single-coder analysis, we employed multiple strategies. First, we kept a detailed audit trail documenting all analytical decisions, including initial code development, code refinements, and theme emergence. Second, preliminary themes and interpretations were iteratively discussed with two senior researchers familiar with qualitative security research, who reviewed the codebook, coding examples, and emerging themes, providing critical feedback that strengthened our analysis. Regular discussions among the whole research team validated our interpretations and minimised bias. This combination of transparency strategies addresses concerns about single-coder bias while

Table 1: Stakeholder Level Research Design Summary

Stakeholder level	No of Sessions	Length of session	No of Questions
policymakers	1-day workshop	87 minutes	17
Policy Promoters	1-day workshop	125 minutes	17
Policy Implementers (12 companies)	4 workshops in 1-month	75 minutes	16

Table 2: Participant Demographics Summary

Stakeholder by Levels	Gender	Total
policymakers	2W / 4M	6
Policy Promoters	3W / 8M	11
Policy Implementers (12 companies / SMEs)	5W / 23M	28

preserving the interpretive depth characteristic of qualitative inquiry.

To maintain anonymity while allowing immediate contextualisation of the quotes in our analysis, we use the following participant identifiers: policymakers (PM.A-PM.F, 6 participants), policy promoters (PP.A-PP.K, 11 participants), and policy implementers (PI.A-PI.L, 12 companies). We aggregate PI perspectives at the company level and consider responses from transcripts of focus group discussions (quotes marked with the participant attribution, e.g., PI.A). In the presentation of the results of our analysis in the remainder of the paper, we mark quotes taken from the response sheets with the suffix "RS" in the participant attribution (quotes marked with the suffix "RS" in the participant attribution, e.g., PI.A-RS).

3.5 Ethics and Data Handling

This study was approved by our institutional ethics board at the University of Southern Denmark in accordance with GDPR requirements. Participants signed the informed consent (see appendix A.5) and confirmed they were 18 years of age or older. All names and identifiers were removed; pseudonyms were used in transcripts. Audio recordings were encrypted and deleted after transcription. We manually checked automated transcriptions for any remaining personal information.

4 RESULTS

Our study of 45 participants across three stakeholder levels identifies common concerns and notable differences in cybersecurity perceptions within Denmark's defence sector. We organise results along three research questions: perceptions and current posture (RQ1), preparedness relative to international benchmarks (RQ2), and global emerging threats (RQ3).

4.1 RQ1: Perceptions and Current Posture in Denmark

4.1.1 Perception of Cost vs. Investment. A dominant divide emerged in how stakeholders perceive cybersecurity. PPs and PIs characterise it primarily as a financial burden, while PMs view it as a strategic investment. PP.H explained: *"our members, small businesses, view this as a financial cost, most of them, because it doesn't generate any value to their bottom line [...] it's not a necessity for their customers. So [...] they have a lot of awareness. They know this is important, but they do not invest in it because it doesn't generate any value to their business."* Most PIs perceive cybersecurity as a financial burden driven by regulatory compliance or cyber insurance requirements. PI.B noted: *"We have a cybersecurity insurance and we are able to keep that up. And every day they do a requirement review where we actually have to comply to the new standards."* Yet, two PMs took balanced stances, seeing cybersecurity as both cost and investment. PM.F stated: *"It's both a cost, but it's also an investment for them."* Some PMs indicated that compliance-driven implementations could "enable business opportunities," suggesting regulatory requirements may act as catalysts for re-framing security measures. The relationship between organisational size and cybersecurity perception emerged as significant, with defence sector PIs representing an interesting exception—several PPs indicated these organisations could meet high standards when motivated by sector requirements, suggesting sector-specific pressure may override general SME resource constraints.

4.1.2 The Herring Effect: Low Awareness and Training. Denmark's cybersecurity posture shows growing awareness alongside persistent challenges. PMs and PPs agree that PIs recognise cyber threats but adopt reactive rather than proactive stances, relying on collective anonymity rather than individual defence mechanisms. PP.J metaphorically described: *"the smaller companies are aware of the cybersecurity threat [...] they are actually more like working like a school of herrings. Just so that they are not to be the ones attacked by the shark."* This reactive stance seems to stem from multiple barriers: resource limitations, awareness gaps, and difficulties navigating complex regulatory frameworks. PIs reinforced these challenges, with PI.D-RS listing: *"Resources and prioritization, expertise & responsibility, in sourcing or on-site consultants."* Despite various awareness initiatives, substantial knowledge gaps remain. PM.D characterised general cybersecurity knowledge in Denmark as "way too low," while PPs noted an awareness paradox—extensive resources exist, that said, "overload of options" may paradoxically inhibit engagement, suggesting information abundance without effective guidance functions as a barrier rather than an enabler.

Regarding formal training programs, only three participating PIs (PI.A, PI.I, PI.L) have implemented them. Most PIs (PI.B to PI.H, PI.J to PI.K) confirmed having no formal awareness training structures, relying instead on informal communications during meetings and lunches. PI.D-RS wrote: *"Raise awareness: verbal communication on phishing attempts. No training."* Some PIs believed their small size made informal communication sufficient. PI.F explained: *"we're only seven people. We're not 300 people [...] we're not LEGO [...] we're a small organisation."* When asked about colleague awareness levels, only PI.A reported high cybersecurity awareness; others indicated

colleagues ranged from low awareness to not taking cybersecurity seriously.

4.1.3 Resource Constraint and Capability Gaps. A striking contrast emerged in stakeholder characterisations: PPs and PIs provided extensive accounts of insufficient resources to implement comprehensive cybersecurity measures, while PM commentary was notably sparse—only two participants briefly acknowledged PI insufficient preparedness, suggesting divergent concern levels across stakeholder groups. The skill shortage appeared particularly acute. PM.D noted: *"we lack skilled cybersecurity programmers and practitioners."* PP.E reinforced: *"I'll make a bit harsh statement and say we simply do not have skilled people, enough skilled people in Denmark."* This shortage extends beyond technical expertise to encompass legal, business, and strategic cybersecurity knowledge. PP.B summarised: *"you need people from different backgrounds actually [...] ones who are thinking from the law perspective [...] from the business perspective and those who are thinking from the technical perspective."* Only PI.B confirmed having a dedicated IT team in-house. Most PIs outsource cybersecurity to external companies or rely on a single computer-savvy person, often the CEO. PI.C-RS wrote: *"IT and hardware is not in-house."* PI.I explained consequences: *"The biggest challenge is the absence of structured cybersecurity governance. Employees have too much freedom to install software, increasing potential risks."* Education gaps arose as a contributing factor, with PPs agreeing on misalignments between academic programs and industry requirements. PP.E stated: *"Very few people understand the standards and how to implement them [...] these things need to be baked into education."* Despite challenges, PPs provide "knowledge support for SMEs", including "helping SMEs with standards" and "guides for risk management," translating complex requirements into actionable steps.

4.1.4 Perceived Threats.

Threat Perception Gaps. A concerning pattern emerged around threat visibility and perception. PMs and PPs characterised PIs as possessing surface-level awareness, failing to grasp the full extent of the threat landscape. PIs underestimate themselves as targets or stepping stones to larger corporations and underestimate threat levels. PM.F noted: *"Most of them actually don't consider it a big threat before it happens,"* suggesting a reactive rather than a proactive threat posture. PMs suggested cybersecurity threats connect with other threats, requiring an integrated rather than an isolated conceptualisation.

Threat Actor Landscape. Relative consensus emerged regarding threat actors. PMs and PPs agree that all companies face risks from both state and non-state actors, though PMs and PPs consistently identified "non-state actors as the main threat," primarily through ransomware and opportunistic attacks. PI analyses focused predominantly on non-state actor threats. However, PMs and PPs reported that state actors also target PIs. PM.B explained: *"There's also the risk [...] mainly state actors who would look into their products, try to steal their technologies, but also try maybe to implement switches, kill switches [...] so that they can shut off their systems."*

Table 3 summarises primary threats identified based on frequency: phishing (concern for all participants), malicious and non-malicious insider threats (PMs worried about malign actors; PPs and PIs focused on insecure behavioural components), ransomware, hacking, malware, physical access to hardware (PI concern only), and third-party threats (all participants, with PMs emphasizing vendor lock-in, PPs focusing on supply chain visibility). Additionally, four primary weaknesses emerged from focus group discussions, ranked by frequency: regulatory complexities and governance gaps; human factors; technological dependencies and legacy system weaknesses; and geographical weaknesses.

Regulatory Complexities and Governance Gaps. The regulatory environment poses particular challenges for PIs. Regulatory complexity functions as vulnerability through compliance confusion. The complexity of "navigating NIS2 compliance" and the broader "regulatory burden" suggest that frameworks intended to enhance security may paradoxically undermine it by overwhelming PI response capacity. Only three PIs have a NIS2 implementation (PI.A, PI.B, PI.G). Three PIs were implementing ISO 27001 (PI.L, PI.B) or 9001 (PI.H). PI.K described: *"NIS2 and ISO 27001 is a demand in many tenders. The standards are heavy for PIs. The risk is that a consultant fills in the blanks and doesn't get any wiser."* PI.B added: *"based on NIS2 requirement, we used plus 500 hours just to understand what it is [...] and used a lot of money on implementing new things."* PPs present detailed perspectives, reflecting difficulties PIs face in understanding and applying cybersecurity guidelines. Governance gaps compound these challenges. The unclear role of SAMSIK (Danish Centre for Cybersecurity) leaves stakeholders uncertain about coordination points and responsibilities. While centralization of incident reporting emerged as strength, PM.E noted: *"when you have incidents you have everything at the Center for Cybersecurity [...] one institution having focus on all incidents,"* but PM.B argued: *"There's very much information going into them but not something coming out [...] very difficult to get in contact [...] very reluctant to come back with information."* PP.E questioned: *"What are their role and responsibilities? That is still not clear since 2011."* No PI mentioned SAMSIK when asked about challenges or guidance sources, underscoring the need for communicating SAMSIK's role and scope to PIs. A reluctance to share vulnerability information emerged as a pattern among PMs and PPs, who cited the "fear of sanctions" from government entities, creating disincentives to transparent reporting. This fear creates an imbalance in information, as policymakers lack access to comprehensive information about real-world security challenges.

More broadly, PMs and PPs identified a lack of a comprehensive ecosystem strategy, leaving initiatives operating without clear integration. The assessment that Denmark had an "immature cybersecurity ecosystem" suggests foundational structures remain underdeveloped. Communication failures characterised the landscape: "confusion or lack of awareness about the cybersecurity strategy" indicated that even when policies existed, dissemination and internalisation remained problematic. PPs and PMs assessed the Danish national cybersecurity strategy (2022-2024) as having fundamental implementation deficits, describing it as too theoretical and noting that deployment has not occurred despite existing frameworks. This gap manifested in sectoral fragmentation, varying municipal practices, resource-limited public agencies, and overwhelmed PIs. Multiple PMs and PPs suggested strategies become obsolete before implementation, strongly favouring shorter cycles (1 year versus

Table 3: Primary Cybersecurity Threats Identified by Participants

Threat Type	Key Concerns	Representative Quotes
Phishing	This was a key concern for all participants. Even PMs experienced phishing.	*'...we are the most targeted institution in Denmark...where they get all these kinds of emails with wrong spelling, they should delete them and so on...'*–PM.A
Malicious and non-malicious insider threats	While all participants share this concern, their specific focus varied. PM primarily worried about malign actors, while PP and PI focused on the insecure behavioural component.	*'The biggest risk comes from internal ignorance rather than intentional harm. While we do not believe we are being directly targeted, the risk of being randomly affected by an attack remains high.'*–PI.G
Ransomware	This was a concern for all participants.	*'I think we have a case last week with a company who had all of their data captured by a ransomware attack here in Denmark.'*–PM.B
Hacking	This was a concern for all participants. PMs and PPs highlighted hacking in general. PIs main fear is being hacked one day.	*'I think the main threat is definitely hacking, getting into their systems.'*–PM.F *'It's probably that we get hacked. So we can't access our systems.'*–PI.F
Malware	This was a concern for all participants. PMs and PPs highlighted malware in general. PIs' concerns ranged from customers, suppliers, to external actors, for example, malware in files from customers and suppliers	*'the sleeping malware.'*–PI.E
Physical access to hardware	This was a key concern for PIs only.	*'Physical access to hardware. (For e.g., access to lab, lock screens, access to office)'*–PI.D
Third-party threat	For all participants, this was a key concern. PMs emphasised vendor lock-in, while PPs focused on supply chain visibility, e.g., Microsoft. PIs concerns ranged from suppliers to customers	*'I think from my perspective, it would be now a supply chain network. So if one of our suppliers were attacked, how that actually compromised our ability to deliver products'*–PI.B. *'Supply chain risks are also significant, subcontractors with access to our systems could introduce vulnerabilities.'*–PI.G

typical 3-5 years) because cyber threats evolve rapidly. PP.C stated: *"done beats perfect."* The fast pace of disruptive technologies like AI and quantum computing compounds this challenge.

Human Factors. Human factors emerged as critical vulnerabilities often overshadowed by technological concerns. Beyond the skilled professional shortage, PIs described insufficient training and awareness programs and "low general awareness" leaving even well-intentioned users poorly equipped to recognize and respond to threats. Behavioural vulnerabilities appear rooted in organisational incentive structures. PPs described "productivity-security tension, noting cybersecurity strategies vs incentives (productivity) often conflict." PP.B illustrated how productivity pressures override security protocols: *"we spend resources defending confidential data, then you have something like ChatGPT come along with people just uploading all the data willingly because it helps them solve problems and the incentives of work."* This tension reflects broader patterns where organizations exhibit "overemphasis on cost" discouraging security investments lacking clear ROI. Educational gaps extend beyond workforce training to fundamental deficits in the education system. PMs and PPs described inadequate focus on "diversity in cybersecurity skills" and "fragmentation in cybersecurity education," which are undermining comprehensive workforce development. Danish cultural characteristics emerged as potentially double-edged factors. Multiple participants from PP characterized Denmark as trust-based and open posture society," facilitating collaboration but creating security vulnerabilities. PP.D stated the "culture was too much trusting," potentially leading to insufficient scepticism regarding insider threats or social engineering. PPs noted that "the public sector failing" to set an example undermined the development of a security culture. PP.A highlighted varied security levels: *"security levels vary, with some public agencies maintaining high security and others falling behind."* This inconsistency introduces additional risks when working across sectors. PP.E expressed: *"We must make*

cybersecurity not just technical but diverse, integrating it across different areas of education and work environments." Additionally, PP.D stated: *"there's too much trust and willingness to look at the insider from a cultural perspective,"* leaving organisations vulnerable to insider threats. Many organisations overlook risks posed by employees unintentionally compromising sensitive data. PI.H shared: *"We have a lot of unspoken trust in our workforce."* Reliance on ageing leadership with limited cybersecurity knowledge compounds issues. PM.B noted: *"board members tend to be older white males [...] who might not be well-versed in technologies and have maybe a rudimentary understanding of cybersecurity threats."* PIs also reported organisational issues, including poor security leadership. PI.D noted: *"Most people are aware, but it's not a priority."*

Technological Dependencies and Legacy System Weaknesses. A concerning pattern emerged around cybersecurity positioning in technological and legacy systems. PPs characterised "cybersecurity as an afterthought in development," suggesting that security considerations are retrofitted rather than built in, creating vulnerabilities that are addressed only after system operation. There is growing concern about adopting new trends. PP.B mentioned: *"We sometimes blindly follow new trends, like AI, without considering the risks,"* exposing organisations to unforeseen vulnerabilities in haste to stay current. The technological monoculture risk was pronounced. PPs and PMs described an "over-reliance on specific technologies," specifically identifying "Microsoft technologies" as potential single points of failure. One participant noted "monoculture risk" observing that "heavy dependence on certain widely-used technologies" could result in "widespread and severe consequences" if compromised. Legacy system integration posed particular challenges. PPs described how "integration of old and new tech poses vulnerabilities," with "some systems having 20 to 30 years" operational lifespans while "IT infrastructure operated on 5 year" refresh cycles. This temporal misalignment created "different shearing layers of technology" complicating security maintenance. PP.E remarked: *"now it's the civilian market that is way ahead,"* terming it the "exponential shift," widening the gap in adoption and security measures. Emerging technologies also raised concerns, with all stakeholders mentioning "quantum technology threats" and "AI" risks, suggesting disruptive technologies might outpace defensive capabilities.

Geographical Weaknesses. Denmark's international positioning creates specific vulnerabilities. PMs and PPs noted Denmark's "forward-leaning Ukraine posture changes threat dynamics," potentially increasing Denmark's profile as a target. Geographic dispersion creates particular concern. The Kingdom of Denmark includes the Faroe Islands and Greenland. PMs and PPs observed increased cybersecurity risks in Denmark's remote areas, driven by fragile infrastructure and heightened geopolitical interest in the Arctic. Risk of foreign interference in Greenland and the Faroe Islands appeared especially pronounced, with concerns about the potential to "interfere in elections." PM.B explained that Greenland's status outside EU cybersecurity frameworks creates significant potential for "foreign interference" due to coordination gaps. PP.D stated: *"The infrastructure in Greenland and the Faroe Islands is incredibly fragile,"* complicating SME security efforts. While geographical weakness navigation was prominent in PM and PP groups, PIs did not mention this issue.

Participants characterized overall cybersecurity posture through varied lenses: "confusing," "scary," "messy," and dependent on perspective. PP.C summarised SME posture: *"I would say in short that it's confusing, insecure and messy."*

4.2 RQ2: Preparedness Relative to International Benchmarks

Focus group discussions revealed three key dimensions: perceived preparedness, international benchmarks, and NATO's impact on Danish PIs.

4.2.1 Perceived Preparedness. Responses varied significantly across participant groups. PMs generally reported adequate organisational readiness, whereas PPs and PIs predominantly reported insufficient preparedness. Preparedness levels appeared low, with PPs and PMs noting companies' "lack of contingency plans" and that they are "definitely not equipped" for cyber incidents. However, two PMs optimistically "observed Denmark is getting better," suggesting gradual improvement despite concerning baselines. PMs and PPs offered nuanced assessments of Denmark's international standing. PP.B indicated "Denmark ranked about 35th" in cybersecurity, though multiple participants emphasised that it depends on "what other nations you are comparing to." Some characterized "Denmark as advanced compared to many others" while noting it might lag behind leading nations.

The digitalisation factor appeared crucial to preparedness assessments. PP.G noted: *"Denmark is a frontrunner in being a digital society."* Participants suggested "Denmark as a digital society makes cybersecurity harder" because "high digitalisation increases fragility" by creating more attack surfaces. PM.C admitted: *"Denmark is highly digitised, but that makes us more vulnerable."* This led some PPs and PMs to characterise comparisons with less-digitalised nations as an unfair comparison." Specific comparisons emerged with Nordic and European peers. Regarding Norway, participants indicated "Norway is still working on NIS1," suggesting Denmark was further along in implementation. One participant summarised: "Denmark is not far behind others", while noting "we're doing quite well" in specific areas like the banking sector and cybersecurity. Interestingly, PMs noted interest from "international delegations" in certain Danish approaches, particularly digital "E-gov," suggesting some aspects attracted positive international attention. Despite middling overall rankings, PMs identified specific domains of excellence. The "banking sector is very advanced" in cybersecurity, suggesting sectoral rather than universal capabilities.

PIs showed the most diversity in responses, ranging from comprehensive preparedness to minimal preparation. Only PI.A reported being prepared: *"We are prepared. Different backups, awareness, and security systems. And we have NIS2."* However, PI.F stated: *"Not very prepared, but we have a back-up of the system every 15 minute. And we have a cyber insurance."* The defence sector faced particular R&D challenges. Multiple PPs emphasised the defence sector's "lack of investment in R&D" undermines technological capability development. One participant noted "technological capability is key for defence," nevertheless, current investment levels appeared insufficient to maintain a competitive advantage.

Response tools exist but face utilisation challenges. PPs and PMs mentioned a "developed warning system" and "various tools

that can help" PIs respond to incidents. Denmark has "SAMSIK" as "single point of entry for all cyber incident response" covering both "military and civilian side," suggesting structural response capability. However, limitations emerged: "[SAMSIK] is quite a small setup," which constrains its capacity. Moreover, while "an established hotline" existed to support PIs, PMs noted "nobody calls them," suggesting awareness gaps or concerns about using government resources. Various "initiatives targeting SMEs" existed, though PPs hinted at a need to find a "sweet spot for SMEs" that balances security objectives with resource realities. Notably, PMs and PPs indicated PIs could achieve high security standards when properly motivated. The observation that "SMEs within the defence sector meet high standards" when "driven by sector requirements" suggests the challenge may be less about absolute incapacity and more about prioritisation and motivation.

4.2.2 International Frameworks: NIS2 & NIST CSF 2.0 Divergence. Our findings suggest complex relationships between international frameworks and Danish defence sector practices.

A key finding centred on NIS2's scope: while "NIS2 does not apply to defence" is not explicit, its supply chain provisions and customer demand create indirect obligations. PM and PP participants noted "our customers need to be NIS2 compliant," effectively requiring defence PIs to implement NIS2 measures regardless of formal applicability. PIs must ensure that both infrastructure and products meet NIS2 standards, creating a "two-sided" compliance requirement. PPs suggested this dual requirement adds considerable complexity. PP.E described "understanding NIS2 for infrastructure and product sides" as potentially confusing, particularly among "small companies unsure about NIS2 relevance."

The primary driver for NIS2 compliance appeared to be "demand from customers and regulations" rather than intrinsic security motivations, suggesting market pressures function as more potent compliance drivers than regulatory mandates for organisations outside the directive's direct scope. PPs expressed generally positive views of NIST, with PP.E characterising it as a "kind of holy grail of many standards." However, NIST's origins create challenges for European organisations. PMs and PPs noted "divergence between European and international frameworks" that "creates issues for companies operating on both sides of the Atlantic." This transatlantic regulatory divergence has proved particularly problematic for defence contractors engaged in NATO-related work, where compliance with both European and American standards may be required. PMs and PPs identified a clear issue with 'increased cooperation between the US" to harmonise or coordinate requirements. In contrast, PIs did not mention these specific challenges but did express overwhelming burdens in implementing them. PIs focused on compliance with either one or both standards, including NIS2 and ISO certifications (9001, 27001). PI.L stated: *"Priority no. 1 [is] ISO 27001."*

4.2.3 Impact of NATO Membership on Danish PIs. NATO membership creates both advantages and complications for Danish PIs. On the positive side, PMs characterized it as "huge advantage to be a NATO member," primarily due to market access: "membership created NATO business opportunities" enabling Danish companies to "cooperate on developing common strategies" and "access a big market to sell it." Several PMs noted NATO engagement facilitated knowledge transfer, with Denmark "Learning from NATO activities" and gaining Influence through NATO on quantum technologies" and other emerging domains. PP.E stated: *"We learn a lot by participating in many NATO activities, for example, NIAG studies or IST panels [...] we look into how quantum [...] will look like for the future [...] goes into NATO as a recommendation."* However, NATO membership also introduced complexity through the aforementioned divergence in standards and the previously outlined geopolitical factors, such as Denmark's stance on Ukraine.

4.3 RQ3: Emerging Global Threats

Supply chain security emerged as threat. PMs and PPs described "dependence on a small number of IT providers" creating "centralization of risk," particularly in public sector's heavy "reliance on a small group of IT providers." This concentration creates systemic vulnerability where compromise of a single provider could cascade across multiple dependent organisations. Another important aspect that the PM and PP groups raised was the over-reliance on foreign technology providers. PM.C highlighted dependence on foreign providers, particularly in critical infrastructure sectors: *"we don't have any Danish solutions, we are dependent a lot on other countries to deliver solutions to some of the most vulnerable parts of our society."* This concentration of risk was emphasized by PP.A: *"we are relying too much on our Microsoft partner; if they get hit, we all suffer."* Divergent perspectives emerged only in the PM group regarding solutions to this dependency. While some participants advocated for increased domestic capacity, others supported international collaboration.

PM.B mentioned: *"We don't need Danish companies to deliver all solutions. We need European or transatlantic companies."* PMs appeared divided on whether Denmark should invest in developing a domestic cybersecurity industry. One perspective emphasised the "lack of Danish cybersecurity companies" as problematic, advocating for an industrial policy to build indigenous capabilities. An alternative perspective questioned whether Denmark's small market could support a full-spectrum cybersecurity industry, instead advocating for "an opportunity for Danish niche players" focused on areas of distinctive competence. More broadly, participants identified "supply chain risks in cybersecurity" and suggested "insufficient focus on securing the supply chain," particularly among smaller companies in supply chains that lack the resources for robust security. This challenge was notably absent from PI discussions.

4.4 Additional Insights: Cross-Sector Collaboration

Our exploration of cross-sector collaboration revealed a paradoxical landscape: while PMs and PPs acknowledged these collaborations' importance and cited specific successful examples, they simultaneously characterised overall collaboration levels as insufficient. PM.B remarked: *"We have a high degree of consultation in policy making in Denmark [...] that serves everybody's best interests."* However, multiple PMs and PPs characterized collaboration levels as inadequate, describing "low level of collaboration," "insufficient

public-private collaboration," and "limited cross-sector communication." Participants described isolated, episodic collaborations rather than systematic partnership structures.

PMs and PPs described "institutional fragmentation in the public sector" and "fragmented cybersecurity efforts" undermining coherent action. The challenge of "difficult to figure out what are the different roles" suggests ambiguity about responsibilities and coordination mechanisms. Bureaucratic processes further complicate collaboration. PMs and PPs noted "challenges with bureaucratic processes" that might slow or discourage partnership formation, particularly for PIs less equipped to navigate administrative complexity.

Several participants referenced the "triple helix" model, which describes collaboration among academia, industry, and government. PM.B commented: *"I think we actually pride ourselves in having this triple helix approach with the academia, government, and the businesses all working together."* But they suggested implementation remains incomplete. One noted "triple helix model requires understanding," implying conceptual clarity about the model's operation may be lacking. The academic component appeared particularly fragmented. PPs described "fragmentation in cybersecurity education" and "lack of coordination between universities" resulting in "overlapping efforts and gaps in critical areas." This educational fragmentation undermines workforce development and potentially limits academia's contribution. Success metrics also appeared unclear, with PP.B noting *"KPIs determine success of collaboration,"* but without evident consensus on appropriate indicators. All PMs and PPs noted that while there is a willingness to collaborate, communication breakdowns and bureaucratic complexities limit effectiveness. PIs particularly struggle to engage with existing initiatives due to time and resource constraints. PPs emerged as important facilitators of collaboration and knowledge intermediaries. Various funding and support initiatives were noted. However, PMs and PPs indicated that these "initiatives are not well-coordinated" and "they're not communicated very well," suggesting that fragmentation extends even to support mechanisms intended to address it. The governance of these initiatives appeared unclear. Despite overall concerns, PMs and PPs acknowledged specific Danish advantages for collaboration. Several characterised Denmark as "having very good collaboration" in specific project contexts and described the ecosystem as "broad and connected." The assessment that collaboration is "easier for small countries" suggests Denmark's size might facilitate network formation.

5 DISCUSSION

In this paper, we investigated mental models across three stakeholder groups (policymakers, policy promoters, policy implementers) regarding Denmark's cybersecurity posture. Our analysis revealed misalignments that explain persistent gaps between policy intent and security outcomes in defence supply chains dominated by SMEs.

5.1 RQ1: How do policymakers (PM), policy promoters (PP), and policy implementers (PI) perceive Denmark's current cybersecurity posture?

5.1.1 Cost vs. Investment. **The Gap:** PMs view cybersecurity as a strategic investment while PPs and PIs frame it primarily as a compliance obligation.

PIs' insurance-heavy approach may be economically rational given their constraints [119]. Research on optimal cybersecurity resource allocation shows that when vulnerability remains low, relying primarily on insurance with minimal upfront investment is mathematically optimal [74]. However, our data reveals a critical gap: while optimisation models prescribe dynamic, periodic reassessment, SMEs treat insurance as static protection without the continuous adaptation required for cost-effectiveness [74]. This creates what researchers term optimisation without adaptation"-adopting economically sound strategies but failing to maintain the conditions under which they remain optimal [74]. Furthermore, another gap emerged: cyber insurance might create a false sense of security for PIs. Despite literature on cyber insurance benefits [129], potential adverse effects of cyber insurance adoption remain understudied and merit further investigation [1].

The prevalent cost-oriented framing of cybersecurity among SMEs contradicts a growing body of evidence that security investments can generate positive returns through enhanced customer trust [73], regulatory compliance enabling market access [11], reduced breach-related costs [48, 53], and competitive advantages, including cyber-resistance capabilities, innovation protection, and product differentiation [63]. However, as Beautement et al. [9] note, these benefits often manifest indirectly and over extended timeframes, making them difficult for resource-constrained SMEs to perceive and prioritise.

Practical Implications:

- *Re-frame security as business enabler.* Our findings that defence sector PIs achieved high security standards when motivated by sector requirements suggest demonstrating substantial business value can overcome resource constraints. For PMs and PPs: (1) communicate investment rationale in financial terms that stakeholders understand, (2) develop case studies demonstrating how security investments enabled specific business opportunities (e.g., contracts requiring NIS2 compliance, entering markets with stringent security requirements like NATO).
- *Incremental investment model.* The "all or nothing" perception may particularly discourage PIs. For PMs: develop graduated security frameworks defining minimum viable security (tier 1), enhanced security (tier 2), and advanced security (tier 3), with clear articulation of business benefits at each level and interim goals rather than overwhelming targets. This approach, similar to accessibility [1] and capability [2] maturity models, provides interim goals rather than distant, overwhelming targets.

[1] https://www.w3.org/TR/maturity-model/ Accessibility Maturity Model
[2] https://https://c2m2.doe.gov/

The cost/investment framing disconnect explains why technically sound policies fail - they assume a shared understanding of security's strategic value that empirically does not exist. By documenting this specific misalignment through stakeholder interviews and connecting it to economic optimisation theory, we provide actionable insight: cybersecurity awareness and education campaigns must address SMEs' cost-minimisation mental model.

5.1.2 The Herring Effect: Collective Risk Perception and Awareness Paradox. **The Gap:** PMs and PPs recognise that cybersecurity awareness and education in Denmark is low and needs improvement. In contrast, PIs take a reactive stance, investing little in formal training and relying instead on informal communication and "collective anonymity" rather than proactive security measures. Although cyber threats are widely acknowledged, many still struggle to take action [116]. This directly challenges the foundational assumption in security awareness research that providing information drives behaviour change. Our findings align with recent work on security fatigue [122, 125] and choice overload [110], demonstrating that the problem is not information scarcity but information overload coupled with decision paralysis [29, 122]. This has critical implications for the design of security awareness interventions. Like their international counterparts, Danish SMEs recognise the reality of cyber risks but often wait to invest in security until after a breach occurs. They cite concerns about costs, complex standards, and an unclear return on investment. These findings are not unique to Danish SMEs. Welsh SMEs experience similar challenges, facing limited awareness, difficulty affording protective measures, and trouble finding skilled professionals, even with the support of public programs [103]. Only 3 of 12 participating SMEs implemented formal awareness programs despite widespread recognition of threats. Most relied on informal lunch conversations and ad hoc warnings. This isn't ignorance - it's a deliberate choice reflecting resource constraints and organisational culture [6, 61, 62, 94, 104]. Participants explicitly stated their small size made informal communication "sufficient." This reveals a gap between expert assumptions about necessary security infrastructure (formal training programs, documented procedures) and SME operational reality (trust-based, informal, resource-constrained).

Practical Implications:

PP Design contextualised micro-learning modules (5-10 minutes) addressing specific organisational and comprehensive training programs. Research on corporate training demonstrates that micro-learning accommodates time constraints while building capability incrementally. Modules should be: immediately actionable, searchable by topic for just-in-time access, and also delivered via mobile platforms [59].

PP Create peer learning networks leveraging the "advanced SMEs" our participants identified. Design structured mentorship programs in which successful SMEs share their approaches with peers. Research on communities of practice shows practitioners learn more effectively from peers facing similar challenges than from external experts.

PM Implement decision-support systems that filter and prioritise from overwhelming options. Rather than comprehensive security guides, design tools provide contextually appropriate recommendations based on organisation size, sector, and threat profile. The UK's Cyber Essentials [82] offers precedent: five focused controls that provide a baseline of security without overwhelming organisations.

PI Our study findings led to the creation of a mapping tool specifically designed for assessing vulnerabilities and capabilities in small and medium-sized enterprises (SMEs). This tool addresses the unique assessment challenges we identified by offering a user-friendly framework that enables SMEs to systematically evaluate their cybersecurity readiness without requiring extensive technical expertise.

This finding demonstrates how mental model elicitation reveals implementation failures invisible to policymakers. PMs assume awareness initiatives reach SMEs, but our PI interviews reveal a disconnect: SMEs know resources exist but cannot navigate them or lack time to engage.

5.1.3 Human Factors: Trust-Based Culture as Double-Edged Sword. **The Gap:** PMs and PIs focus on technical or regulatory solutions. At the same time, PPs see human behaviour and organisational incentives as the real problem. Each stakeholder identifies different root causes (systemic education gaps vs. productivity pressures vs. workplace culture), revealing a disconnect in how they frame and would address cybersecurity vulnerabilities. Danish SMEs practice what Kocksch and Jensen term "living with insecure IT" [61] - not through ignorance but through deliberate choices balancing security, productivity, and cultural norms. Ethnographic research documents Danish workers sharing passwords to avoid repeatedly washing greasy hands (prioritizing workflow efficiency), practising "a little but not a lot" rule-breaking (maintaining flexibility), and relying on Jantelov (cultural modesty norms) that prevent identifying valuable IT assets as doing so would constitute "bragging [61]." This reveals sophisticated informal security practices that formal policies may fail to recognize or support. Furthermore, participants noted that employees were uploading confidential data to "ChatGPT" because it helped them solve problems and address the "incentives of work." This exemplifies the persistent "knowing is not the same as doing" paradox - employees understand security requirements but violate them when productivity pressures demand [104]. Research demonstrates that this isn't malicious intent but reflects conflicts between security rules and the work-efficiency requirements that time-critical tasks necessitate bypassing [104]. Recent research on security culture [6, 61, 62, 94, 104] emphasises the importance of aligning security measures with organisational values, but few studies examine how national culture shapes these dynamics. Pollini et al.'s empirical evidence from healthcare organisations reveals that a strong cybersecurity culture in healthcare doesn't always mean rule compliance; work efficiency pressures lead to well-intentioned violations, such as password sharing for patient care or using personal devices for work data [94].

Practical Design Implications: For All Stakeholders:

- Design security interventions leveraging rather than contradicting trust-based culture. Rather than imposing external controls, build cybersecurity communities where employees

feel collective responsibility. Research on religious communities' millennia of managing human fallibility suggests moving beyond rule-based compliance toward fostering belonging through shared cybersecurity values that employees genuinely commit to rather than merely obey [104]. Implementation: Regular storytelling about security successes, positive messaging rather than fear appeals, and rituals that make secure behaviours habitual through repeated, supported practice.

- Redesign security policies acknowledging "broken world thinking." Recognise that cybersecurity in resource-constrained SMEs operates not through comprehensive fixes but through situated improvisation and enduring partial insecurity. Design policies that accommodate legacy technologies that cannot be updated, workflows that require temporary rule-breaking, and financial constraints that make "waiting things out" more feasible than implementing complete overhauls. This means accepting "good enough" security rather than aspirational visions, leaving organisations feeling perpetually inadequate [61].
- Create contextual security guidance integrated into workflows. Rather than separate security training, embed security prompts directly into the tools used for actual work. For the ChatGPT example: Design prompts for uploading files that ask, "Does this contain confidential data?" with one-click alternatives (internal LLM, anonymisation tools). This reduces friction between productivity and security rather than forcing binary choices.

This finding provides the strongest support for our contribution that high-trust cultural contexts create distinct mental model dynamics compared to low-trust settings. By connecting our empirical observations to ethnographic research on Danish workplace practices, we demonstrate how cultural context fundamentally shapes what security interventions will succeed. We also draw on theory related to values-based security communities to support our findings. The practical implication - security design must be culturally adapted - represents actionable insight for both researchers and practitioners working in diverse cultural contexts.

5.1.4 Regulatory Complexity: Well-Intentioned Frameworks, Unintended Consequences. **The Gap:** PMs acknowledged that PIs may be overwhelmed by regulatory burdens, but there's a disconnect: PMs don't fully understand the extent of this burden, while PPs are aware of it but lack the ability to change regulatory frameworks in order to help PIs. This suggests that PMs may underestimate how excessive regulatory burden can actually undermine the security objectives these regulations are meant to achieve. Regulatory compliance interfaces represent critical points of interaction where policy meets practice. Poor usability of compliance requirements creates what researchers term "compliance theatre" organizations satisfy formal requirements while neglecting substantive security [69, 97]. This resonates with extensive research on regulatory burden and recent works [84, 85] specifically on cybersecurity compliance challenges. The design of compliance guidance, assessment tools, and reporting interfaces directly affects whether regulations improve security or merely create an administrative burden.

Despite NIS2 not formally applying to many defence organisations, PIs reported spending "plus 500 hours just to understand what it is" and hiring consultants to "fill in the blanks," creating a financial burden without necessarily improving security understanding. One PI described the risk: "consultant fills in the blanks and [SME] doesn't get any wiser." This reveals a critical implementation failure - compliance activities occur, but learning and capability-building do not. Also, as PP remarked, customer demand forces these companies to implement the regulations. One issue that resonated with participants across all three stakeholder groups was the lack of well-defined roles and responsibilities for key national entities (such as the Danish CFCS). This can hinder exchanges regarding incidents.

Practical Design Implications:

PM Design plain-language compliance guides following established readability principles. Current guidance uses legal and technical language inaccessible to SME audiences. Redesign should include explanations of what must be done (not just what is required), worked examples showing compliant implementations in realistic scenarios, and decision trees to help organisations determine the applicability of requirements. The UK Financial Conduct Authority[3] offers useful precedent for embedding plain language principles into regulatory frameworks.

PM Create subsidised compliance assistance programs, recognising that some SMEs lack the capacity to interpret requirements regardless of guidance quality. Design includes: free initial compliance assessments, voucher programs for security consulting, "compliance workshops" where SMEs receive expert guidance [6].

PM We recommend that the respective entities sharpen their public profiles and establish (a) materials PPs can distribute to members about the roles, responsibilities, and services offered to PIs and (b) clear paths for communication in case PIs encounter incidents and make sure that PIs know about these paths.

PP Design compliance mapping tools showing relationships between overlapping frameworks (NIS2, ISO 27001, NIST, NATO). The tool should identify: controls that satisfy multiple frameworks simultaneously, conflicts requiring divergent implementations, and gaps where one framework requires controls not addressed by others. This reduces perceived burden by showing that compliance work has multi-framework benefits.

This finding supports our contribution by showing how mental model misalignment at the PM level (underestimating implementation burden) cascades into policy failures. By documenting specific implementation challenges and proposing design solutions grounded in readability research and regulatory best practices, we demonstrate how mental model elicitation enables evidence-based policy refinement.

5.1.5 Perceived Threat. **Threat Perception Gap:** On the one hand, PMs and PPs see a comprehensive, interconnected threat landscape requiring proactive vigilance, and see PIs as underestimating both the threat landscape and their own value as targets. On the other

[3] https://handbook.fca.org.uk/latest-news/news-details/86215d4b-1dfe-4a8b-aa8b-5e88a937fe20 for more details, see the FCA's approach.

hand, PIs feel they are unlikely targets, suffer from "threat fatigue," in which everything becomes a threat, and take a reactive rather than proactive stance, considering threats serious only after incidents occur.

Threat Actors Landscape Gap: PIs predominantly focus only on non-state actors (ransomware, opportunistic attacks), while PMs and PPs recognise that both state actors (stealing technologies, implementing kill switches) and non-state actors pose significant threats to PIs.

Regarding technological dependencies and integration challenges, previous research positions cybersecurity as a problem requiring coordination across multiple tiers, where individual efforts may fall short; collaborative decision-making and coordinated investments among partners can help avoid both under- and over-investment [22, 113]. Our research extends these results by identifying issues such as vendor lock-in, legacy system integration, and swift adoption of AI, which contribute to complex, system-wide vulnerabilities.

Practical Implication for SME-focused interventions:

(1) Sector-specific threat intelligence: The finding that threat perceptions vary by sector suggests value in tailored threat intelligence. For PPs: Develop sector-specific threat intelligence briefings for SMEs. These should: focus on threats actually observed in similar organisations (not theoretical possibilities), provide concrete indicators of compromise that SMEs can monitor, suggest proportionate controls appropriate to the threat level, and be delivered via multiple channels (email alerts, web portal, association newsletters, webinars) to maximise reach.
(2) Risk prioritisation matrices (Risk assessment planning): To help SMEs move from threat identification to prioritised action, for PPs and Academics: Develop simple risk matrices plotting threats by likelihood and impact. Also, tools for mapping threats, risks, and vulnerabilities to their respective capabilities. The matrix should: use plain language descriptions of likelihood ("attacks of this type happen to businesses like yours several times per year" rather than statistical probabilities), describe impact in business terms ("could force temporary closure" rather than technical consequences), map available controls to specific risks enabling direct action, and update quarterly to reflect evolving threat landscape.
(3) Crisis prioritisation guides (Formal incident response plans): PMs and PPs mentioned PIs lacking or having no formal plans for crisis, and even well-prepared organisations may struggle to prioritise actions during active incidents. For PPs: Develop incident-specific response prioritisation guides. For common threat types (ransomware, DDoS, data breach), these would include: immediate actions (within the first hour), short-term actions (within the first 24 hours), medium-term recovery steps (within the first week), and criteria for when to seek external assistance.

5.2 RQ2: International Preparedness - The Digitalisation Paradox

The Gap: PMs reported adequate organisational readiness while PPs and PIs indicated insufficient preparedness. More fundamentally, Denmark's advanced digitalisation creates a paradox: high digital maturity increases attack surfaces faster than security capabilities can protect them.

Our findings suggest that digitalisation without proportional security investment creates systemic vulnerability. This has implications for designing digital services and assessing technology adoption strategies. Denmark ranks approximately 35th globally in cybersecurity, but this numerical positioning may obscure nuanced realities. Participants characterised comparisons with less digitally advanced nations as "unfair" because extensive digitalisation creates unique attack surfaces that less digitally advanced nations do not face. This suggests cybersecurity rankings may confound capability with exposure - highly digital countries appear weaker, not from poor capability but from greater vulnerability surface. Additionally, sectoral variation proved striking: the banking sector demonstrated advanced cybersecurity while the defence sector lacked R&D investment. This indicates that Denmark possesses technical capacity and expertise but lacks coordination mechanisms to ensure consistent application across sectors.

Practical Design Implications:

PM Design strategic frameworks translating sectoral successes across domains. Banking sector achievements could serve as a model for minimum security standards in other critical sectors. Implementation requires accounting for varying resource levels - graduated standards appropriate to organisational capacity rather than uniform requirements.
PM Leverage Denmark's small size advantage for coordination. Small countries can achieve closer coordination and more agile decision-making than larger nations. Design formalised mechanisms facilitating knowledge sharing between advanced and developing sectors through structured peer learning networks.

This finding supports our contribution by revealing how the level of digitalisation fundamentally shapes the threat landscape in ways that current preparedness assessments fail to capture. By documenting this digitalisation paradox and proposing design solutions for cross-sector knowledge transfer, we provide actionable insight for both national cybersecurity strategy and international benchmarking methodologies.

5.3 RQ3: Emerging Threats - Supply Chain Blind-spots

The Gap: PMs and PPs viewed supply chain security and foreign technology dependence as critical threats, while PIs were notably absent from these discussions, suggesting they do not share these concerns or perceive relevance to their operations.

Supply chain security requires coordination across organisational boundaries, making it fundamentally a socio-technical challenge. Design of supplier assessment tools, risk communication interfaces, and collaborative security mechanisms directly impacts whether supply chain vulnerabilities can be identified and mitigated [76]. Furthermore, literature on supply chains highlights the importance of visibility, a unified language or taxonomy, and coordinated investments. In areas where domestic capabilities are lacking,

policy measures can help by promoting diversified systems, creating exit options, and ensuring transparency in contracts [22, 75, 123].

The supply chain threat perception gap reveals a hierarchical gap in threat visibility: threats visible at the policy level remain invisible at the implementation level. This isn't ignorance but reflects different operational realities: PMs consider strategic vulnerabilities across national infrastructure, while SMEs focus on immediate operational threats. Neither perspective is wrong, but misalignment means SMEs do not implement protective measures against systemic threats they do not perceive as relevant [115].

This finding supports our contribution by documenting a specific mental model gap (threat visibility) with direct security implications. By proposing design solutions that enable SMEs to operationalise supply chain security despite lacking strategic threat visibility, we demonstrate how understanding mental model gaps enables targeted interventions that bridge policy-implementation divides.

Practical Design Implications: For Policymakers: Regulatory sandbox approach: To test new requirements before full implementation. A promising approach involves implementing regulatory sandboxes, controlled environments where emerging technologies like AI and machine learning can be tested under regulatory supervision, enabling both innovators and regulators to collaboratively understand associated risks and compliance requirements. PMs can establish regulatory sandboxes where volunteer organisations test new requirements and provide feedback [72]. This approach, pioneered in financial services regulation, enables regulators to assess whether requirements are interpretable, implementable, and effective before broad roll-out. Participating organisations might receive temporary immunity from enforcement while testing new approaches. Furthermore, establishing international working groups to align AI-related cybersecurity standards could facilitate cross-border cooperation and promote secure technological innovation while maintaining necessary regulatory agility and security standards [72].

For Policy Implementers: Design supplier security assessment frameworks involving cross-functional teams (procurement, IT, operations) to evaluate vulnerabilities collaboratively. The framework should be publicly available, proportionate to risk (more stringent for higher-risk suppliers), and aligned with relevant standards (ISO 27001, NIS2) to leverage existing supplier investments. Tool development: Create risk prioritisation matrices that plot threats by likelihood and impact, using plain-language descriptions and business-term impacts rather than technical jargon.

For Policy Promoters: Design collective supply chain security initiatives. Given that many SMEs use common suppliers, organise pooled resources for supplier assessment (reducing individual burden), collective negotiation with suppliers on security requirements (achieving better terms through volume), and shared threat intelligence about supplier compromises. This recognises supply chain security as a collective action problem where individual efforts prove insufficient.

5.4 Cross-Sector collaboration and support for PIs

Our findings revealed that while Denmark has strong collaborative traditions and successful isolated examples, there's a systemic failure to move from episodic, project-based partnerships to coordinated, sustainable structures, compounded by institutional fragmentation, unclear roles, poor communication of support initiatives, and lack of agreed-upon success metrics that collectively prevent effective cross-sector cybersecurity collaboration.

Across all participants, a persistent pattern emerged: reluctance to share vulnerability information due to fear of sanctions. This creates a problematic information imbalance where policymakers lack access to complete information about real-world security challenges, undermining evidence-based policy development [42, 49]. Information sharing requires trust, and trust requires appropriate socio-technical infrastructure. Design of protected disclosure mechanisms, anonymous reporting systems, and information sharing platforms directly impacts whether information flows necessary for collective security can occur [26, 50, 124]. Research reveals counter-intuitive dynamics: when firms share security information, each firm reduces its own security spending, even as the collective security level increases. However, without appropriate incentive mechanisms, firms face strong temptations to free-ride - benefiting from others' shared information while withholding their own. Our findings empirically validate this theoretical prediction: stakeholders recognised the value of information sharing but reported that it doesn't occur due to misaligned incentives [50].

Practical Design Implications:

PM Design protected disclosure frameworks with formal safe harbour provisions. Specify: what types of disclosures are protected (self-discovered vulnerabilities, near-miss incidents, compliance challenges), what protection is provided (immunity from enforcement, reduced penalties), and time limits for disclosure to receive protection. Such frameworks exist in aviation safety and healthcare domains and could be adapted to cybersecurity. Critical design requirements: codified in regulation (not informal policy), providing legal certainty, well-publicised so organisations know it exists, consistently applied, building confidence.

PM Establish Information Sharing and Analysis Centres (ISACs), facilitating voluntary exchange of cybersecurity threat data. Research shows that mandated information sharing increases total social welfare but requires enforcement mechanisms to prevent defection. Design should include sector-specific nodes enabling tailored threat intelligence relevant to particular industries [50].

PM Research-practice translation service: To bridge the gap between research publication and practitioner adoption, for PPs and academic research centres: establish dedicated translation services that convert academic research into practitioner-accessible formats. This might include: plain-language summaries of relevant research, webinars presenting research findings to practitioner audiences, tool-kits and templates operationalising research recommendations, and case studies showing research-backed approaches in practice. Such services often prioritise accessibility over relevance; practitioners cannot apply research they cannot understand.

PM Collaborative education programs: To address the skills shortage while building connections, for academics and PPs: Develop collaborative education programs. These might include:

executive education programs designed jointly by academics and practitioners; micro-credentials in specific cybersecurity topics that combine academic rigour with practical relevance; capstone projects in which student teams solve real industry problems; and apprenticeship models that combine academic learning with practical experience.

This cross-cutting finding demonstrates how mental model elicitation reveals systemic governance failures. By documenting the information-sharing dilemma, we illustrate its complexities. We also propose design solutions grounded in game theory and regulatory precedent from other domains. Additionally, we show how HCI design principles, such as trust and appropriate incentives, apply to national cybersecurity governance challenges.

5.5 Contributions for the HCI community

Our findings advance HCI cybersecurity research in three ways:

- Cultural context matters: Most security design research originates in low-trust contexts (especially the US) [77, 78]. Our findings demonstrate that trust-based cultures create fundamentally different dynamics, requiring culturally-adapted interventions. This challenges the universal applicability of existing security design principles and suggests the need for comparative security culture research.
- Mental Model elicitation as design method: While prior mental models research focused on individual users and usability, we demonstrate how systematic elicitation across stakeholder levels reveals governance-to-implementation gaps that explain policy failures. This methodological contribution suggests mental model research should expand from individual cognition to organisational and inter-organisational levels.
- Optimisation without adaptation: We identify a novel pattern in which SMEs adopt economically sound strategies (insurance-heavy approaches) but fail to maintain the dynamic adaptation needed for those strategies to remain optimal. This contributes to understanding security decision-making under resource constraints and suggests the need for easy-to-use decision-support tools enabling continuous strategy reassessment.

5.6 Limitations

While we applied methodological rigour, we acknowledge certain limitations in our study. The voluntary nature of participation may have introduced some selection bias, potentially over-representing individuals and organisations more engaged with cybersecurity issues. Recruiting diverse participants, especially women, was challenging despite efforts at demographic balance. Furthermore, we only included participants from Denmark in this study. Therefore, our results cannot be assumed to generalise beyond this context and replicating our methods in different cultural contexts, in particular, a more gender-balanced sample and investigations in non-WEIRD contexts, might prove very valuable future work. Additionally, despite our English proficiency requirement, language barriers may have subtly influenced the depth of expression for some participants. Furthermore, our sample, while diverse in organisation affiliation, may not fully represent the breadth of perspectives across Denmark. While our defence sector focus enabled depth, it may limit transferability to other contexts. Defence sector organisations face distinctive pressures (national security imperatives, classification requirements, NATO standards) that may not apply elsewhere.

5.7 Future Works

- Future research could explore how NIS2 requirements serve as catalysts for enhanced cyber awareness, which would provide valuable insights for policy development and strategies to promote organisational compliance. In addition, understanding how the EU's NIS2 directive will affect Danish SMEs requires investigation into rule-based NIS2 clash with Danish trust cultures, appropriate implementation models that minimise cultural disruption, and monitoring mechanisms respectful of Scandinavian egalitarianism. Research should examine what support infrastructure Danish SMEs need to comply with evolving regulatory requirements.
- Future research on employee training - Studies by Rader and Wash [100] and Das et al. [24] showed that stories and social influence transmit security lessons more effectively than formal training. In addition, Renaud and Dupuis [104] research proposes learning from an unexpected source: religious practices. Religions have millennia of experience in understanding human nature and guiding behaviour despite people's tendency to err. Storytelling and scenario-based training, which have been successful in religion, would be promising in the cybersecurity context. This can be empirically tested in such high-trust societies.
- Future research should include: direct engagement with SME decision-makers, particularly in micro-enterprises (<10 employees) that face the most severe resource constraints, longitudinal studies tracking how perspectives and practices evolve over time, and cross-national comparative studies examining whether our findings generalise beyond Danish contexts.

6 Conclusion

This paper examines cybersecurity mental models across three stakeholder groups in Denmark's defence sector: policymakers, policy promoters, and policy implementers. Our findings reveal shared concern for supply chain cybersecurity alongside key divergences in how responsibilities, threats, and readiness are interpreted. While all stakeholders recognised the urgency of cybersecurity, SMEs faced significant implementation barriers that policymakers often underestimated. Effective cybersecurity requires addressing these structural and human challenges through implementable strategies, regulatory frameworks that acknowledge differential organisational capacity, trust-based information-sharing mechanisms, systematic human capacity development, and explicit coordination structures. Although our study focuses on Denmark's defence sector, the challenges identified—implementation gaps, SME resource constraints, human factors, regulatory complexity—resonate across nations. Our contribution lies in demonstrating how mental-model elicitation can inform socio-technical governance practices beyond end-user interventions.

Acknowledgments

We thank all participants across Denmark's defence policymakers, industry experts and SME representatives for generously contributing their invaluable insights. This work was funded by the Danish Industry Foundation under grant number 2023-0393. This work was supported by the Topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by the KASTEL Security Research Labs.

References

[1] Rodney Adriko and Jason R. C. Nurse. 2024. Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms. *Digital Threats* 5, 3, Article 25 (Oct. 2024), 39 pages. doi:10.1145/3676283

[2] Erdinc Akyildirim, Thomas Conlon, Shaen Corbet, and Yang Greg Hou. 2024. HACKED: Understanding the stock market response to cyberattacks. *Journal of International Financial Markets, Institutions and Money* 97 (2024), 102082.

[3] A. Alexander, C. Blome, M.C. Schleper, and S. Roscoe. 2022. Managing the 'new normal': the future of operations and supply chain management in unprecedented times. *International Journal of Operations & Production Management* 42, 8 (2022), 1061–1076.

[4] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. *Mental Models of Security Risks.* Springer Berlin Heidelberg, Berlin, Heidelberg, 367–377. doi:10.1007/978-3-540-77366-5_34

[5] C. Warren Axelrod. 2015. Reducing software assurance risks for security-critical and safety-critical systems. *Journal of Strategic Security* 8, 4 (2015), 75–90. doi:10.5038/1944-0472.8.4.1476

[6] Maria Bada and Jason R.C. Nurse. 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security* 27, 3 (July 2019), 393–410. doi:10.1108/ics-07-2018-0080

[7] O. Bak, S. Shaw, C. Colicchia, and V. Kumar. 2023. A systematic literature review of supply chain resilience in small–medium enterprises (SMEs): a call for further research. *IEEE Transactions on Engineering Management* 70, 1 (2023), 328–341.

[8] Murat Bayraktar and Neşe Algan. 2019. The Importance Of SMEs On World Economies. In *International Conference on Eurasian Economies 2019*, Vol. 12. Eurasian Economists Association, Skopje, North Macedonia, 56–61. doi:10.36880/c11.02265

[9] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and Angela Sasse. 2016. Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 253–270. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

[10] Lukasz Bednarski, Samuel Roscoe, Constantin Blome, and Martin C. Schleper. 2023. Geopolitical disruptions in global supply chains: a state-of-the-art literature review. *Production Planning & Control* 36, 4 (Dec. 2023), 1–27. doi:10.1080/09537287.2023.2286283

[11] Michael Benz and Dave Chatterjee. 2020. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business horizons* 63, 4 (2020), 531–540.

[12] Terry Besser and Nancy Miller. 2001. Small Business Community Values & Their Relationship to Management Strategies. *The Journal of Socio-Economics* 30, 6 (2001), 221–241.

[13] Sandor Boyson. 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation* 34, 7 (July 2014), 342–353. doi:10.1016/j.technovation.2014.02.001

[14] Gary L. Brase, Eugene Y. Vasserman, and William Hsu. 2017. Do different mental models influence cybersecurity behavior? Evaluations via statistical reasoning performance. *Frontiers in Psychology* 8 (2017), 1929. doi:10.3389/fpsyg.2017.01929

[15] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie S Downs, and Saranga Komanduri. 2011. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26.

[16] Karoline Busse, Julia Schäfer, and Matthew Smith. 2019. Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 117–136. https://www.usenix.org/conference/soups2019/presentation/busse

[17] L. Jean Camp. 2006. *Mental Models of Security.* Technical Report. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735 Working paper, SSRN Abstract ID 922735.

[18] L. Jean Camp. 2009. Mental Models of Privacy and Security. *IEEE Technology and Society Magazine* 28, 3 (2009), 37–46.

[19] CBS Wire. 2021. Small and medium-sized businesses make up 99 percent of Denmark's businesses, but are hardly represented at universities. https://cbswire.dk/small-and-medium-sized-businesses-make-up-99-percent-of-denmarks-businesses-but-are-hardly-represented-at-universities/ Accessed August 29, 2025.

[20] Centre for Cyber Security (CFCS), Denmark. 2024. The cyber threat against Denmark 2024. CFCS website (PDF report). https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs---the-cyber-threat-against-denmark-2024.pdf Published September 20 2024. Provides an updated national cyber threat assessment with categories and levels (espionage, crime, activism, destructive attacks, terrorism)..

[21] Kam-Fung Cheung, Michael G.H. Bell, and Jyotirmoyee Bhattacharjya. 2021. Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review* 146 (Feb. 2021), 102217. doi:10.1016/j.tre.2020.102217

[22] Alessandro Creazza, Claudia Colicchia, Salvatore Spiezia, and Fabrizio Dallari. 2021. Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal* 27, 1 (May 2021), 30–53. doi:10.1108/scm-02-2020-0073

[23] Dansk Industri. 2019. *SMV'er er Danmarks Vækstlokomotiver.* Dansk Industri. https://www.danskindustri.dk/di-business/arkiv/nyheder/2019/2/smver-er-danmarks-vakstlokomotiver/ Accessed: 2025-08-29.

[24] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 143–157. https://www.usenix.org/conference/soups2014/proceedings/presentation/das

[25] Department for Business, Energy & Industrial Strategy. 2023. BEIS small and medium enterprises (SMEs) action plan: 2022 to 2025. https://www.gov.uk/government/publications/beis-small-and-medium-enterprises-sme-action-plan-2022-to-2025/beis-small-and-medium-enterprises-smes-action-plan-2022-to-2025-accessible-webpage Accessed August 29, 2025.

[26] Jorge Augusto Depetris. 2002. The Regulatory Craft Controlling Risks, Solving Problems, and Managing Compliance. *Documentos y Aportes en Administración Pública y Gestión Estatal: DAAPGE* 2, 3 (2002), 135–137.

[27] Digitaliseringsstyrelsen. 2023. *Digital sikkerhed i danske SMV'er 2023.* Technical Report. Digitaliseringsstyrelsen. https://www.sikkerdigital.dk/Media/638326091245131541/Digital%20sikkerhed%20i%20danske%20SMV'er%202023_endelig0310-a.pdf Accessed: 2025-07-11.

[28] Myriam Dunn-Cavelty and Manuel Suter. 2009. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection* 2, 4 (Dec. 2009), 179–187. doi:10.1016/j.ijcip.2009.08.006

[29] Jessica Maria Echterhoff, Aditya Melkote, Sujen Kancherla, and Julian McAuley. 2024. Avoiding Decision Fatigue with AI-Assisted Decision-Making. In *Proceedings of the 32nd ACM Conference on User Modeling, Adaptation and Personalization* (Cagliari, Italy) *(UMAP '24)*. Association for Computing Machinery, New York, NY, USA, 1–11. doi:10.1145/3627043.3659569

[30] European Commission. 2019. *2019 SBA Fact Sheet — Denmark.* Technical Report. European Commission. https://single-market-economy.ec.europa.eu/publications/sba-fact-sheet-denmark-2019_en Based on Eurostat Structural Business Statistics. SMEs account for 99.7% of enterprises, 60.8% of value added, and 64.1% of employment in Denmark.

[31] European Parliament and Council. 2022. 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). https://eur-lex.europa.eu/eli/dir/2022/2555/oj Official Journal of the European Union L 333/80.

[32] European Union Agency for Cybersecurity (ENISA). 2021. *ENISA Threat Landscape for Supply Chain Attacks.* Technical Report. European Union Agency for Cybersecurity, Athens, Greece. doi:10.2824/168593

[33] Morten Falch, Henning Olesen, Knud Erik Skouby, Reza Tadayoni, and Idongesit Williams. 2022. Cybersecurity in SMEs in the Baltic Sea Region. In *ITS 31st European Conference 2022.* International Telecommunications Society, International Telecommunications Society, Gilford, NH, 1–20.

[34] Morten Falch, Henning Olesen, Knud Erik Skouby, Reza Tadayoni, and Idongesit Williams. 2023. Cybersecurity Strategies for SMEs in the Nordic Baltic Region. *Journal of Cyber Security and Mobility* 11, 6 (Jan. 2023), 727–754. doi:10.13052/jcsm2245-1439.1161

[35] M. Faruquee, A. Paulraj, and C. A. Irawan. 2023. A typology of supply chain resilience: recognising the multi-capability nature of proactive and reactive contexts. *Production Planning & Control* 35, 12 (2023), 1503–1523. doi:10.1080/09537287.2023.2202151

[36] Linda Finlay. 2002. "Outing" the researcher: The provenance, process, and practice of reflexivity. *Qualitative Health Research* 12, 4 (2002), 531–545.

[37] European Union Agency for Cybersecurity, V. Paggio, G. Bafoutsou, and A. Sarri. 2021. *Cybersecurity for SMEs – Challenges and recommendations.* Publications Office, Athens, Greece. doi:10.2824/770352 Report on cybersecurity challenges and recommendations for small and medium-sized enterprises in the European

Union.
[38] European Union Agency for Cybersecurity (ENISA). 2024. ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Accessed: 2025-07-10.
[39] Organisation for Economic Co-operation and Development (OECD). 2020. Enhancing the contributions of SMEs in a global and digitalised economy. https://www.oecd.org/industry/smes/. Accessed: 2025-07-10.
[40] Agency for Science and Cybersecurity Denmark (ASCD). 2020. Final Report: Strengthening the Cybersecurity of Danish SMEs. https://www.ascd.dk/publications/sme-cybersecurity-report. Accessed: 2025-07-10.
[41] Canadian Business for Social Responsibility. 2003. Engaging Small Business in Corporate Social Responsibility. A Canadian Small Business Perspective on CSR.
[42] Esther Gal-Or and Anindya Ghose. 2005. The economic incentives for sharing security information. *Information Systems Research* 16, 2 (2005), 186–208.
[43] M. R. Galbreth and M. Shor. 2010. The Impact of Malicious Agents on the Enterprise Software Industry. *MIS Quarterly* 34, 3 (2010), 595–612. doi:10.2307/25750693
[44] Anisha Banu Dawood Gani, Yudi Fernando, Shulin Lan, Ming K. Lim, and Ming-Lang Tseng. 2022. Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data Systems* 123, 3 (Dec. 2022), 843–861. doi:10.1108/imds-05-2022-0313
[45] Wang Gao, Jiajia Wei, Hongwei Zhang, and Haizhen Zhang. 2024. The higher-order moments connectedness between rare earth and clean energy markets and the role of geopolitical risk: New insights from a TVP-VAR framework. *Energy* 305 (2024), 132280.
[46] Catalin Gheorghe and Oana Panazan. 2025. Geopolitical risk contagion across strategic sectors: Nonlinear evidence from defense, cybersecurity, energy, and raw materials. *PLoS One* 20, 9 (2025), e0330557.
[47] Robin Bender Ginn and Omkhar Arasaratnam. 2024. Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects. https://openssf.org/blog/2024/04/15/open-source-security-openssf-and-openjs-foundations-issue-alert-for-social-engineering-takeovers-of-open-source-projects/ Joint alert on social engineering attacks targeting open source projects.
[48] Lawrence A. Gordon and Martin P. Loeb. 2002. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* 5, 4 (Nov. 2002), 438–457. doi:10.1145/581271.581274
[49] Lawrence A Gordon, Martin P Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, 6 (2003), 461–485.
[50] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22, 6 (2003), 461–485. doi:10.1016/j.jaccpubpol.2003.09.001
[51] Margareta Heidt, Jin P. Gerlach, and Peter Buxmann. 2019. Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers* 21, 6 (2019), 1285–1305. doi:10.1007/s10796-019-09959-1
[52] D. M. Herold and L. Marzantowicz. 2023. Supply chain responses to global disruptions and its ripple effects: an institutional complexity perspective. *Operations Management Research* 16 (2023), 2213–2224.
[53] C. Derrick Huang and Ravi S. Behara. 2013. Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics* 141, 1 (2013), 255–268. doi:10.1016/j.ijpe.2012.06.022 Meta-heuristics for manufacturing scheduling and logistics problems.
[54] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion
[55] Mikkel Storm Jensen. 2018. Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle. *Scandinavian Journal of Military Studies* 1, 1 (2018), 1–18. doi:10.31374/sjms.3
[56] P. N. Johnson-Laird. 1980. Mental Models in Cognitive Science. *Cognitive Science* 4, 1 (1980), 71–115.
[57] Panagiotis Katrakazas and Spyros Papastergiou. 2024. A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience. *Businesses* 4, 2 (2024), 225–240.
[58] Hidayet Keskġn, Canan Ġentürk, Onur Sungur, and Hakan M Kġrġġ. 2010. The importance of SMEs in developing economies. In *2nd International Symposium on Sustainable Development*. International Burch University, Sarajevo, Bosnia and Herzegovina, 183–192.
[59] Iacovos Kirlappos, Adam Beautement, and M. Angela Sasse. 2013. "Comply or Die" Is Dead: Long Live Security-Aware Principal Agents. In *Financial Cryptography and Data Security*, Andrew A. Adams, Michael Brenner, and Matthew Smith (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 70–82.
[60] Jeroen Klomp. 2025. The impact of the Hamas-Israel conflict on the US defense industry stock market return. *PloS one* 20, 2 (2025), e0314677.
[61] Laura Kocksch and Torben Elgaard Jensen. 2024. The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small- and Medium-Sized Enterprises. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW2 (Nov. 2024), 1–17. doi:10.1145/3686893
[62] Katarina Kostelić. 2024. Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach. *Games* 15, 2 (April 2024), 13. doi:10.3390/g15020013
[63] Dejan Kosutic and Federico Pigni. 2020. Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy* 43, 1 (10 2020), 28–36. arXiv:https://www.emerald.com/jbs/article-pdf/43/1/28/1316921/jbs-06-2020-0116.pdf doi:10.1108/JBS-06-2020-0116
[64] Richard A. Krueger and Mary Anne Casey. 2002. *Designing and Conducting Focus Group Interviews*. Sage, Thousand Oaks, CA.
[65] Richard A. Krueger and Mary Anne Casey. 2014. *Focus Groups: A Practical Guide for Applied Research* (5th ed.). SAGE Publications, Thousand Oaks, CA.
[66] T. J. Kull, J. Kotlar, and M. Spring. 2018. Small and medium enterprise research in supply chain management: the case for single-respondent research designs. *Journal of Supply Chain Management* 54 (2018), 23–34.
[67] Rajesh Kumar and Ranjith Mallipeddi. 2022. Cybersecurity challenges in Industry 4.0 and 5.0: Human-centric security governance. *Journal of Manufacturing Systems* 64 (2022), 324–337. doi:10.1016/j.jmsy.2022.07.003
[68] Rajesh Kumar Singh, Ruchi Mishra, Shivam Gupta, and Archana A. Mukherjee. 2023. Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda. *Computers & Industrial Engineering* 175 (Jan. 2023), 108854. doi:10.1016/j.cie.2022.108854
[69] Catherine Liston-Heyes and Luc Juillet. 2022. What has become of the audit explosion? Analyzing trends in oversight activities in the Canadian government. *Public Administration* 100, 4 (2022), 1073–1090.
[70] Zokir Mamadiyarov, Shoh Jakhon Khamdamov, Rano Nazarova, Sharofjon Rashidov, Istora Kadirova, Alisher Izzatillayev, and Gulizahro Turayeva. 2025. Cybersecurity Challenges in the Expanding Digital Economy. In *Proceedings of the 8th International Conference on Future Networks & Distributed Systems (ICFNDS '24)*. Association for Computing Machinery, New York, NY, USA, 138–145. doi:10.1145/3726122.3726144
[71] Christopher Manganaro. 2019. Supply chain security starts at home. *Supply Chain Management Review* 23, 4 (July/August 2019), 20–25.
[72] Angelica Marotta and Stuart Madnick. 2025. Analyzing and Categorizing Emerging Cybersecurity Regulations. *ACM Comput. Surv.* 58, 2, Article 51 (Sept. 2025), 36 pages. doi:10.1145/3757318
[73] Kelly D Martin, Abhishek Borah, and Robert W Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of marketing* 81, 1 (2017), 36–58.
[74] Alessandro Mazzoccoli and Maurizio Naldi. 2022-6-16. Optimizing Cybersecurity Investments over Time. *Algorithms.* 15, 6 (2022-6-16), 211–226.
[75] Steven A Melnyk, Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F Chang, and Derek Friday. 2022. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research* 60, 1 (2022), 162–183.
[76] Steven A. Melnyk, Cheri Speier-Pero, and Elizabeth Connors. 2019. Blockchain is vastly overrated; supply chain cyber security is vastly underrated. *Supply Chain Management Review* 23, 3 (May/June 2019), 32–39.
[77] Erin Meyer. 2014. *The Culture Map: Breaking Through the Invisible Boundaries of Global Business*. PublicAffairs, New York.
[78] Erin Meyer. 2015. Building Trust Across Cultures. INSEAD Knowledge. https://knowledge.insead.edu/leadership-organisations/building-trust-across-cultures Accessed October 23, 2025.
[79] N. Moosa, V. Ramiah, H. Pham, and A. Watson. 2020. The origin of the US-China trade war. *Applied Economics* 52, 35 (2020), 3842–3857.
[80] Gareth Mott, Sarah Turner, Jason R C Nurse, Nandita Pattnaik, Jamie MacColl, Pia Huesch, and James Sullivan. 2024. 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. *Journal of Cybersecurity* 10, 1 (07 2024), tyae013. arXiv:https://academic.oup.com/cybersecurity/article-pdf/10/1/tyae013/61182348/tyae013.pdf doi:10.1093/cybsec/tyae013
[81] Douglas W Naffziger, Nazim U Ahmed, and Ray V Montagno. 2003. Perceptions of environmental consciousness in US small businesses: An empirical study. *SAM Advanced Management Journal* 68, 2 (2003), 23.
[82] National Cyber Security Centre. 2025. *Cyber Essentials: Requirements for IT Infrastructure*. Technical Report. UK Government. https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-2.pdf
[83] National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Technical Report NIST CSWP 04162018. National Institute of Standards and Technology. doi:10.6028/nist.cswp.04162018 Accessed July 2025.

[84] Morten Meyerhoff Nielsen, Nuno Ramos Carvalho, Linda Gonçalves Veiga, and Luís Soares Barbosa. 2017. Administrative Burden Reduction Over Time: Literature Review, Trends and Gap Analysis. In *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance* (New Delhi AA, India) *(ICEGOV '17)*. Association for Computing Machinery, New York, NY, USA, 140–148. doi:10.1145/3047273.3047334

[85] OECD. 2020. *Regulatory Impact Assessment*. OECD Publishing, Paris. doi:10.1787/7a9638cb-en

[86] OECD. 2021. OECD SME and Entrepreneurship Outlook 2021. https://www.oecd-ilibrary.org/industry-and-services/oecd-sme-and-entrepreneurship-outlook-2021_97a5bbfe-en

[87] OECD. accessed 2025. Enterprises by business size. OECD website. https://www.oecd.org/en/data/indicators/enterprises-by-business-size.html SMEs defined as fewer than 250 employees, subdivided into micro (fewer than 10), small (10–49), and medium (50–249).

[88] Anna-Marie Ortloff, Jenny Tang, Arthi Arumugam, Daniel Huschina, Lisa Geierhaas, Florin Martius, Luisa Jansen, Kolja von der Twer, Lilly Jungbluth, and Matthew Smith. 2025. Replication:{"No} one can hack my {mind"}-10 years later: An update and outlook on {experts'} and {non-experts'} security practices and advice. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*. USENIX Association, Berkeley, CA, USA, 435–454.

[89] R. Pal, H. Torstensson, and H. Mattila. 2014. Antecedents of organizational resilience in economic crises - an empirical study of Swedish textile and clothing SMEs. *International Journal of Production Economics* 147, PART B (2014), 410–428.

[90] Niki Panteli, Boineelo R. Nthubu, and Konstantinos Mersinas. 2025. Being Responsible in Cybersecurity: A Multi-Layered Perspective. *Information Systems Frontiers* 27, 31 (2025), 31 pages. doi:10.1007/s10796-025-10588-0 Advance online publication.

[91] Sandra Parker, Zhe Wu, and Panagiotis D. Christofides. 2023. Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering* 171 (March 2023), 108169. doi:10.1016/j.compchemeng.2023.108169

[92] Nandita Pattnaik, Jason R. C. Nurse, Sarah Turner, Gareth Mott, Jamie MacColl, Pia Huesch, and James Sullivan. 2023. It's More Than Just Money: The Real-World Harms from Ransomware Attacks. In *Human Aspects of Information Security and Assurance*, Steven Furnell and Nathan Clarke (Eds.). Springer Nature Switzerland, Cham, 261–274.

[93] Haiat Perozzo, Fatema Zaghloul, and Aurelio Ravarini. 2022. CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective. *Complex Systems Informatics and Modeling Quarterly* 0, 33 (Dec. 2022), 53–66. doi:10.7250/csimq.2022-33.04

[94] Alessandro Pollini, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2021. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work* 24, 2 (June 2021), 371–390. doi:10.1007/s10111-021-00683-y

[95] Christophe Ponsard, Jeremy Grandclaudon, and Gautier Dallons. 2018. Towards a Cyber Security Label for SMEs: A European Perspective-. *ICISSP* 4 (2018), 426–431.

[96] Gerald V. Post and Albert Kagan. 2007. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security* 26, 3 (2007), 229–237.

[97] Michael Power. 2003. Evaluating the audit explosion. *Law & policy* 25, 3 (2003), 185–202.

[98] Kendall Prewett, Jacob Phillips, and Ben Jensen. 2022. SolarWinds: A Case Study in Supply Chain Compromise. *Journal of Cybersecurity Education, Research and Practice* 2022, 1 (2022), 1–15.

[99] Maria Puig de la Bellacasa. 2011. Matters of care in technoscience: Assembling neglected things. *Social Studies of Science* 41, 1 (2011), 85–106.

[100] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 6, 17 pages. doi:10.1145/2335356.2335364

[101] Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. 2009. Revealing hidden context: Improving mental models of personal firewall users. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, New York, NY, USA, 1–12.

[102] Fahimeh Raja, Kirstie Hawkey, Steven Hsu, Kai-Le Wang, and Konstantin Beznosov. 2011. Promoting a physical security mental model for personal firewall warnings. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI EA '11)*. Association for Computing Machinery, New York, NY, USA, 1585–1590. doi:10.1145/1979742.1979812

[103] Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, and Chaminda Hewage. 2023. Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights* 3, 2 (Nov. 2023), 100191. doi:10.1016/j.jjimei.2023.100191

[104] Karen Renaud and Marc Dupuis. 2023. Cybersecurity Insights Gleaned from World Religions. *Computers & Security* 132 (Sept. 2023), 103326. doi:10.1016/j.cose.2023.103326

[105] K. Renaud and J. Ophoff. 2021. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People* 1, 1 (2021), 24–46. doi:10.1108/OCJ-03-2021-0004

[106] James Allen Rodger and James A. George. 2017. Triple bottom line accounting for optimizing natural gas sustainability: A statistical linear programming fuzzy ILOWA optimized sustainment model approach to reducing supply chain global cybersecurity vulnerability through information and communications technology. *Journal of Cleaner Production* 142 (Jan. 2017), 1931–1949. doi:10.1016/j.jclepro.2016.11.089

[107] S. Roscoe, E. Aktas, K.J. Petersen, H.D. Skipworth, R.B. Handfield, and F. Habib. 2022. Redesigning global supply chains during compounding geopolitical disruptions: the role of supply chain logics. *International Journal of Operations & Production Management* 42, 9 (2022), 1407–1434.

[108] Johnny Saldaña. 2021. *The Coding Manual for Qualitative Researchers* (4th ed.). SAGE Publications, Thousand Oaks, CA.

[109] Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy* 13, 3 (2015), 80–83. doi:10.1109/MSP.2015.65

[110] Barry Schwartz. 2005. *The Paradox of Choice: Why More is Less*. HarperCollins, New York. Theparadoxofchoice-Whymoreisless.pdf

[111] IBM Security. 2024. IBM X-Force Threat Intelligence Index 2024. https://www.ibm.com/reports/threat-intelligence. Accessed: 2025-07-10.

[112] Daniël Sierat, Ruben Faber, and Bas Schalbroeck. 2024. The XZ-factor: social vulnerabilities in open source projects. https://english.ncsc.nl/latest/weblog/weblog/2024/the-xz-factor-social-vulnerabilities-in-open-source-projects Published by NCSC-NL.

[113] Jay Simon and Ayman Omar. 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research* 282, 1 (April 2020), 161–171. doi:10.1016/j.ejor.2019.09.017

[114] Statistics Denmark. 2024. SMV'er i Danmark – 99,4 % af virksomhederne er små og mellemstore. https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=27734 Accessed: 2025-07-11.

[115] Jan Stentoft and Ole Stegmann Mikkelsen. 2024. Towards supply chain resilience: A structured process approach. *Operations Management Research* 17 (2024), 1421–1443. doi:10.1007/s12063-024-00513-0

[116] Jan Stentoft, Marco Peressotti, Peter Mayer, Kent Adsbøll Wickstrøm, Olivier Schmitt, Vincent Charles Keating, Amelie Theussen, Louise Alison Tumchewics, and Judith Kankam-Boateng. 2025. The relationship between cybersecurity awareness, cybersecurity supply chain risk management and firm performance. *Supply Chain Management: An International Journal* 30, 5 (June 2025), 497–517. doi:10.1108/scm-11-2024-0765

[117] Elizabeth Stobert, David Barrera, Valérie Homier, and Daniel Kollek. 2020. Understanding Cybersecurity Practices in Emergency Departments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. doi:10.1145/3313831.3376881

[118] B. Sullivan-Taylor and L. Branicki. 2011. Creating resilient SMEs: why one size might not fit all. *International Journal of Production Research* 49 (2011), 5565–5579.

[119] Nazim Taskin, Aslı Özkeleş Yıldırım, Handan Derya Ercan, Martin Wynn, and Bilgin Metin. 2025. Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. *Information* 16, 1 (Jan. 2025), 66. doi:10.3390/info16010066

[120] Stephanie Teufel, Bernd Teufel, Mohammad Aldabbas, and Minh Nguyen. 2020. *Cyber Security Canvas for SMEs*. Vol. 1339. Springer International Publishing, Cham, 20–33. doi:10.1007/978-3-030-66039-0_2

[121] David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2 (June 2006), 237–246. doi:10.1177/1098214005283748

[122] John Tierney. 2011. Do You Suffer from Decision Fatigue. *The New York Times* n/a, n/a (17 Aug. 2011), n/a. https://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html

[123] Colin Topping, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid. 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. *Computers & Security* 108 (Sept. 2021), 102324. doi:10.1016/j.cose.2021.102324

[124] Valeria Valdés Ríos, Fatiha Zaidi, Ana Rosa Cavalli, and Angel Rego. 2024. Towards the adoption of automated cyber threat intelligence information sharing with integrated risk assessment. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES '24)*. Association for Computing Machinery, New York, NY, USA, Article 166, 9 pages. doi:10.1145/3664476.3670444

[125] Kathleen D Vohs, Roy F Baumeister, Brandon J Schmeichel, Jean M Twenge, Noelle M Nelson, and Dianne M Tice. 2018. Making choices impairs subsequent self-control: A limited-resource account of decision making, self-regulation, and active initiative. In *Self-regulation and self-control*. Routledge, Abingdon, Oxon,

45–77.
[126] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. doi:10.1145/1837110.1837125
[127] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 309–325. https://www.usenix.org/conference/soups2015/proceedings/presentation/wash
[128] Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2019. "Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300381
[129] Daniel W. Woods. 2023. A Turning Point for Cyber Insurance. *Commun. ACM* 66, 3 (Feb. 2023), 41–44. doi:10.1145/3545795
[130] World Economic Forum. 2025. Global Cybersecurity Outlook 2025. https://www.weforum.org/reports/global-cybersecurity-outlook-2025. Accessed: 2025-07-10.
[131] World Trade Organization. 2016. *World Trade Report 2016: Levelling the trading field for SMEs*. Technical Report. World Trade Organization, Geneva, Switzerland. https://www.wto.org/english/res_e/booksp_e/world_trade_report16_e.pdf
[132] World Trade Organization. 2016. *World Trade Report 2016: Levelling the trading field for SMEs*. Technical Report. World Trade Organization, Geneva. https://www.wto.org/english/res_e/publications_e/wtr16_e.htm
[133] World Trade Organization. 2024. Informal Working Group on Micro, Small and Medium-sized Enterprises (MSMEs). https://icsb.org/ayman-tarabishy/world-trade-organization-and-msmes/ Accessed August 2025.
[134] William Yeoh, Marina Liu, Malcolm Shore, and Frank Jiang. 2023. Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security* 133 (Oct. 2023), 103412. doi:10.1016/j.cose.2023.103412
[135] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3313831.3376570

A APPENDIX

A.1 Definitions of Small and Medium-Sized Enterprises (SMEs)

EU Definition. This paper adopts the European Union's official definition of SMEs, as outlined in the *EU Recommendation 2003/361/EC*.[4] The classification is based on staff headcount, annual turnover, and/or annual balance sheet total, see details in table 4. Article 2 Staff headcount and financial ceilings determining enterprise categories 1. The category of micro, small, and medium-sized enterprises (SMEs) is made up of enterprises that employ fewer than 250 persons and that have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. 2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million. 3. Within the SME category, a microenterprise is defined as an enterprise that employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million. In addition to these financial thresholds, enterprises must be autonomous or fall within specific ownership limits as defined in the official EU guidelines.

UK BEIS Definition. Definition of an SME. The Companies Act 2006 defines a large company as one with a staff headcount of over 250, or with annual turnover exceeding £36m or balance sheet total exceeding £18m. However, in relation to its procurement activities, the UK Government currently defines Small and Medium Enterprises (SMEs) as set out in the table 5 below. SMEs make up an essential component of the private sector business landscape. According to the 2021 Business Population Estimates, there were almost 5.6 million businesses in the UK at the start of 2021. SMEs accounted for 99.9% of the total number. Importantly, SMEs employed 61% of the private sector workforce, totalling 16.3 million employees. They also accounted for 52% of UK plc's turnover, equivalent to £2,300 billion.

British Columbia SMEs Definition. Small and medium-sized enterprises (SMEs) are vital to British Columbia's economy, generating 34% of provincial GDP and 30% of exports in 2023. However, these businesses face growing challenges from expanding mandatory disclosure requirements across federal, provincial, and municipal levels. The total regulatory compliance cost for BC small businesses in 2023, including disclosure requirements, was estimated at $8 billion, with smaller firms bearing significantly higher per-employee costs. Definition. This publication defines a business based on the number of paid employees. Therefore, enterprises without paid employees are not generally included in this publication. In this report, an SME is defined as an enterprise with 1 to 499 paid employees. More specifically:

- a small business has 1 to 99 paid employees;
- a medium-sized business has 100 to 499 paid employees; and
- a large business has 500 or more paid employees.

A.2 Interview Guide Questions for policymakers

Structure. 5 main questions with 2-4 sub questions for Q1 to Q4 and one main question for Q5.

Q1. What is your view on the overall state of cybersecurity in Denmark?

Q1a. Who do you consider to be the main threats in this context?
Q1b. How effectively do you think Denmark is equipped to counter these threats?
Q1c. Do you view cybersecurity primarily as a cost or as an investment?

Q2. What are your thoughts on Denmark's current national cybersecurity strategy?

Q2a. How effective do you find this strategy
- The overall cybersecurity landscape
- Cybersecurity in the public sector
- Cybersecurity for private sector businesses, especially SMEs

Q2b. Are there specific aspects that you think should have been included or highlighted in the strategy?
Q2c. Considering the strategy covers a three-year period, do you believe this time-frame is appropriate?
Q2d. What suggestions do you have for the development of the next national cybersecurity strategy?

Q3. How applicable are the NIS2 and NIST CSF 2.0 frameworks to Denmark's cybersecurity needs?

Q3a. How does Denmark's readiness to manage international cybersecurity threats compare to other countries?

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361

Table 4: EU Definition of SMEs (Recommendation 2003/361/EC)

Enterprise Category	Staff Headcount	Annual Turnover	Annual Balance Sheet Total
Micro	< 10	≤ €2 million	≤ €2 million
Small	< 50	≤ €10 million	≤ €10 million
Medium-sized	< 250	≤ €50 million	≤ €43 million

Table 5: UK BEIS Definition of SMEs (Recommendation 2003/361/EC)

Size of Business	Staff Headcount	Annual Turnover	Balance Sheet Total
Medium	under 250	under £ 50m	under £ 43m
Small	under 50	under £ 10m	under £ 50m
Micro	under 10	under £ 2m	under £ 2m

Q3b. What distinct challenges does Denmark encounter in its cybersecurity initiatives?
Q3c. In what ways does being a member of NATO affect Denmark's cybersecurity strategies?
Q3d. What are the major areas where Denmark's cybersecurity measures fall short compared to other nations?

Q4) What resources do you rely on to inform your policy-making decisions?

Q4a. How dependable are these resources?
Q4b. What methods do you use to address discrepancies between different sources?

Q5) Is there effective Collaboration between the Public Sector, Businesses (especially SMEs), and Academic Institutions?

A.3 Interview Guide Questions for Policy Promoters

Structure. 5 main questions with 1-4 sub questions for Q1 to Q5.

Q1. How do you evaluate the current Danish Cybersecurity posture?

Q1a. What are the key cybersecurity threats you identified?
Q1b. To what extent are the defence sector equipped to defend against these threats?
Q1c. Do you view cybersecurity as a financial cost or a strategic investment?

Q2. What is your perspective on Denmark's national cybersecurity strategy, and how does it impact the defence sector?

Q2a. How effective do you find Denmark's national strategy for:
- i. Influencing the overall industry landscape
- ii. The public sector's influence on private-sector cybersecurity practices?
- iii. Impacting SMEs within the defence sector?

Q2b. Are there specific aspects of cybersecurity that you believe should be emphasised or included in future strategy plans?
Q2c. What is your perspective on the strategic planning (national cybersecurity strategy) time-frame? Should it be longer or shorter?

Q3. How do you perceive the applicability and relevance of international cybersecurity frameworks like NIS2 and NIST CSF 2.0 for the Danish defence sector?

Q3a. How does Denmark's readiness for international cybersecurity threats compare to other nations?
Q3b. What unique challenges are faced by Denmark?
Q3c. How does Denmark's NATO membership impact the cybersecurity strategies of the defence sector?
Q3d. In your opinion, where does Denmark fall short of other countries in terms of cybersecurity?

Q4. Evaluate the level of collaboration between the public sector, private enterprises (especially SMEs), and research institutions.

Q4a. How can SMEs be supported in strengthening cybersecurity practices, e.g., by industry associations or other actors?

Q5. To what extent do Denmark's current policies effectively support SMEs in strengthening their cybersecurity measures to protect against cyber threats and attacks?

Q5a. What are the primary challenges or points of contention/friction between policies and companies regarding cybersecurity regulations, and how can these issues be effectively addressed?

A.4 Interview Guide Questions for Policy Implementers

Structure. We elicited their initial mental models in the morning with 6 main themes with 2-3 questions under each theme. Then the scenario exercises for treatment and finally the Post mental model with 6 main themes with 1 - 3 questions under each theme.

A.4.1 Initial Mental Models - Participant Response Sheet.

1) Understanding the Current Cybersecurity Posture and Practices.

Q1a. According to your current understanding, what are your organisation's cybersecurity practices, and the role cybersecurity plays in daily operations within your organisation?
Q1b. What are the key cybersecurity practices currently implemented, and what are your main concerns or priorities related to cybersecurity?

2) Threats, Vulnerabilities, and Preparedness.

Q1a. What do you perceive as the most significant cybersecurity threats to your organisation?
Q2b. How seriously do you think your colleagues take these cybersecurity threats?
Q2c. In your opinion, how prepared do you feel your organisation is to handle cybersecurity incidents?

3) Training, Awareness, and Communications.

Q3a. In what ways does your organisation train employees and raise awareness about cybersecurity? In your opinion, how effective do you feel these training and awareness efforts are?
Q3b. How are these issues communicated within your organisation? In your opinion, how effective do you feel these communication efforts are?
Q3c. From your experiences, what do you feel is the level of cybersecurity awareness among your peers?

4) Challenges, Approaches, and Risk Assessments.

Q4a. Aside from actual cybersecurity threats you face, what other cybersecurity challenges does your SME face today, and how do you address these challenges in your daily operations?
Q4b. How do you assess and prioritise the cybersecurity threats and challenges and the resulting risks faced by your SME? What factors influence your risk assessment process?

5) Resources, Regulations, Initiatives, and Feedback.

Q5a. Where do you currently search for information and guidance on cybersecurity threats and challenges? How reliable do you feel these sources are?
Q5b. Are you aware of any specific cybersecurity initiatives or regulations that affect your organisation? How do these influence your approach to cybersecurity?
Q5c. How have recent cybersecurity initiatives or regulations affected your SME?

6) Supply Chain Risks.

Q6a. Does your organisation consider supplier-related cybersecurity threats and challenges? If so, what is your organisation's approach to these considerations?
Q6b. Does your organisation consider customer-related cybersecurity threats and challenges? If so, what is your organisation's approach to these considerations?

A.5 Informed Consent

Consent to participate in research and processing of personal data. In connection with the University of Southern Denmark, we want to collect your information. Our researchers are responsible for the protection of sensitive data collected for the use in this research. Participation in our project is voluntary. Data collection takes place through focus group discussions, follow-up interviews, and participant observation. Discussions will be recorded and then transcribed for qualitative analyses. As part of the transcription process, personal data will be removed from the transcripts to ensure that only anonymised data will be analysed.

Purpose of processing information for the project. The purpose of this research is to evaluate the cybersecurity policies and practices in Denmark, to understand the practices and challenges associated with cybersecurity in Denmark. A secondary purpose is to develop the use of scenarios as a method of foresight analysis for cybersecurity in Danish enterprises. The information being processed is: The recordings of the focus groups/discussions and the follow-up interviews for transcription. The transcriptions will then be analysed using qualitative inductive coding. Notes generated from participant observation will be used as a secondary data source to confirm the context and interpretation of the transcripts.

How we use the information. The information is to be processed in accordance with the General Data Protection Regulation (GDPR) art. 6, (1)(a) and art. 9, (2)(a), which cover the rules of consent. The research team will treat the information with confidentiality in accordance with applicable law. We will keep the data secure so that only some researchers taking part in the project, listed above, will have access. The information will only be used for the purposes of the project.

Deletion and storage of your data. We will delete or anonymise the information when it is no longer relevant to keep. The transcription process will always remove identifying information from the transcripts. The anonymised information will be deleted, at the latest, five years after the end of the project, and will therefore be deleted on XX.XX.XXXX. You may withdraw your consent if you wish to have your data deleted earlier before XX.XX.2030, after which it may no longer be possible to remove your data from the dataset due to data deletion. Note that deletion of your data is not possible after it has been anonymised after the transcription process. Please note

- that you can always withdraw your consent earlier before XX.XX.2030, after which it may no longer be possible to remove your data from the dataset due to data deletion, which means the University of Southern Denmark is obligated to delete the information we have collected about you,
- that you have the right to see the data we have about you,
- that you have the right to request the rectification or deletion of data and
- that you have the right to appeal to the Danish Data Protection Agency about the processing of the information via www.datatilsynet.dk.

You always have the option of withdrawing your consent by writing to Peter Mayer.

Disclosure/other purposes. The collected data will only be shared beyond the research team of this project in anonymised form. The data will be stored in encrypted containers at all times after recording until deletion.

Publication. There will be no publication of data in which you can be personally identified. Your personal data is anonymised before being included in the publication of the results of the research. This means that it is not possible to retrieve your information in any publications. Excerpts from the transcripts might be used in publications, in which case attributions with will be made using anonymous identifiers, e.g., Participant 1.

More information. If you have any questions about the research, you can contact at any time either via email at mayer@imada.sdu.dk

or via phone at +4565503531. If you wish to file a complaint about the processing of personal data, you can contact the Danish Data Protection Agency via the University of Southern Denmark.

Declaration of consent.

- I understand that participation in the project is voluntary.
- I have read and understand the informed consent.
- I consent to participate in the research and the processing of the data.
- I understand that the collected data will only be shared beyond the research team of this project in anonymised form.

Date Name Signature

Table 6: Codebook for PolicyMakers

Theme	Category	Code Group	Code
current posture	herring effect	perspectives	like working herring
			SMEs perspectives
			Cybersecurity as an after-thought
			resource and skills constraint
			perception vs reality in threat assessment
			awareness and preparedness
	awareness and training program	awareness and training	low awareness
	regulatory complexity	bureaucratic barrier	overwhelming and confusing
	cost vs. investment	cost	financial burden
			investment
			both cost and investment
	shortage of skilled cybersecurity professionals and education gaps	shortage of skilled cyber professionals	lack of skilled cybersecurity professionals
	capacity and role definition of CFCS	role of CFCS	Why?
			capacity
			roles to SMEs unclear?
	perceived threats	types of threats	state and non-state threat actors
			hacking
			phishing
			ransomware
			malware
			supply chain threats
	technological integration and legacy systems	technology challenges	disruptive technologies like quantum and AI
			over-reliance on specific technologies
			Dependence on a Small Number of IT Providers
	human factor weaknesses	human factors	(insecure) cultural and behavorial practices
			cybersecurity education and skill shortage
			low awareness
			ageing leadership
	geopolitical weaknesses	geopolitical	Ukraine and Russia war
			fragile infrastructure and connectivity in Greenland and the Faroe Islands
collaboration	cross-sector collaboration	public & private collaborations	Coordination and Communication Gaps
			triple helix approach
international frameworks	NIS2 & NIST	benchmarks	Complexities
			divergence in International Standards
	NATO applicability to PIs	Strategic geography and NATO involvement	Vulnerabilities in been NATO member
			Learning and Influence through NATO Membership
			Not deep diving into NATO standards

Continued on next page

Table 7: Codebook for Policy Promoters

Theme	Category	Code Group	Code
current posture	herring effect	perspectives	insecure, confusing & messy
			startup perspectives
			cluster perspectives
			cybersecurity as an afterthought
			resource and skills constraint
			perception vs reality in threat assessment
			awareness and preparedness
	awareness and training program	awareness and training	low awareness
	regulatory complexity	bureaucratic barrier	overwhelming and confusing
	cost vs. investment	cost	financial burden
			investment
			both cost and investment
	shortage of skilled cybersecurity professionals and education gaps	shortage of skilled cyber professionals	lack of skilled cybersecurity professionals
			cybersecurity education
			industry and academia misrequirements
	capacity and role definition of CFCS	role of CFCS	Why?
			capacity
			roles to SMEs unclear?
	perceived threats	types of threats	state and non-state threat actors
			hacking
			phishing
			ransomware
			malware
			supply chain threats
	technological integration and legacy systems	technology challenges	legacy systems
			over-reliance on specific technologies
			Dependence on a Small Number of IT Providers
	human factor weaknesses	human factors	(insecure) cultural and behavorial practices
			cybersecurity education and skill shortage
			low awareness
			ageing leadership
	geopolitical weaknesses	geopolitical	Ukraine and Russia war
			fragile infrastructure and connectivity in Greenland and the Faroe Islands
collaboration	cross-sector collaboration	public & private collaborations	Insufficient public-private collaboration
			triple helix approach
international frameworks	NIS2 & NIST	benchmarks	Complexities
			divergence in International Standards
			limited applicability of NIS2 to defence

Continued on next page

Table 8: Codebook for Policy Implementers

Theme	Category	Code Group	Code
current posture	herring effect	perspectives	awareness and preparedness
			awareness and preparedness
	awareness and training program	awareness and training	low awareness
			high awareness
			medium awareness
			no awareness
			lack of serious engagement from leadership
			informal communication channel
			formal communication channel
			existing awareness and training programs
			no training program
			launching training program
			highly prepared
			moderately prepared
			not prepared
	regulatory complexity	bureaucratic barrier	overwhelming and confusing
			NIS2
			NIST
			ISO 27001
			ISO 9001
			ESG
			GDPR
	cost vs. investment	cost	financial burden
			compliance
			cyber insurance
	shortage of skilled cybersecurity professionals and education gaps	shortage of skilled cyber professionals	lack of skilled cybersecurity professionals
			limited expertise
			dedicated In-house IT team
			outsourcing to external companies
	perceived threats	types of threats	state and non-state threat actors
			hacking
			phishing
			ransomware
			malware
			physical access
			space of operation (constellation takeover)
			We are a vendor to a part in war
			mobile phones usage
			AI
			Machine Learning detection vulnerability
			third party threats
	current practices and preparedness	technology challenges	firewalls
			Microsoft 365
			2FA
			NIS2
			crisis management
			backups
	human factor weaknesses	human factors	(insecure) cultural and behavorial practices
			human error
			open posture
			high trust in the workforce
			poor leadership examples
collaboration	cross-sector collaboration	public & private collaborations	time and resource constraint