Mapping Cybersecurity Practices and Mental Models in Danish Small and Medium Enterprises (SMEs): A Comprehensive Study using Focus Groups[*]

Judith Kankam-Boateng Marco Peressotti Peter Mayer
University of Southern Denmark
jukan24@student.sdu.dk, {peressotti, mayer}@imada.sdu.dk

Abstract

In response to high cyber threats, this paper evaluates the cybersecurity landscape in Danish Small and Medium-sized Enterprises (SMEs) within the defense and IT sectors, mapping perspectives from policymakers, business associations, and SMEs. By integrating quantitative surveys, qualitative focus groups, interviews, and scenario-based simulations, we aim to understand and address the vulnerabilities in these critical sectors. The objective is to evaluate the cybersecurity policies and practices in Denmark, proposing actionable strategies to Danish SMEs making them resilient and contributing significantly to national security. The findings from this study are intended to contribute to the discourse on usable security practices and their implications for business continuity and policy formulation within the SME context.

1 Introduction

Danish Small and medium-sized enterprises (SMEs)[1] in the defense and IT sectors face escalating cybersecurity threats due to their critical roles and strategic data sensitivity [4, 7, 20, 3, 15, 16, 22, 20]. These enterprises, characterized by limited security budgets and infrastructural constraints, are particularly susceptible to cyber-attacks [13, 8, 12, 11]. This study aims to investigate the current cybersecurity practices of these SMEs [18] regarding cybersecurity standards [17, 8, 2] to pinpoint vulnerabilities [5] and develop targeted improvements. To this end, we aim to map the mental models and operational realities of Danish SMEs [19] using a mixed-methods approach and incorporating perspectives from policymakers, business associations, and companies alike.

2 Methodology

The study adopts a mixed-methods approach [6, 1, 21] to provide a holistic view of the cybersecurity posture within Danish SMEs. This approach integrates both quantitative and qualitative methods to capture nuanced insights into the attitudes and perceptions that underpin existing cybersecurity practices. By combining these methods, the study aims to address the following research questions:

RQ1 What are the perceptions of policymakers, policy promoters, and companies regarding Denmark's current cybersecurity stance in the context of its national standards, strategies, and initiatives?

RQ2 How do policymakers, policy promoters, and companies compare Denmark's cybersecurity posture with respect to international standards, strategies, and initiatives, and what are their views on its preparedness against global cybersecurity threats?

2.1 Quantitative Component

A survey will be distributed to 50 SMEs within the defense and IT sectors. This survey aims to gather empirical data on current security processes, adherence to policy, the effectiveness of incident response strategies, and investments in cybersecurity technologies. The data collected will provide a baseline understanding of the cybersecurity practices and challenges faced by SMEs.

[*] This work was partially supported by Industriens Fond, Grant 'Cybersikkerhed og Forretningskontinuitet'.

[1] Small and medium-sized enterprises (SMEs) are defined in the EU recommendation 2003/361. The main factors determining whether an enterprise is an SME are staff headcount either turnover or balance sheet total. The table 1 explain the definitions for SMEs in EU Commission. Under Danish law, there is no special definition for SMEs. Data of the structure of SMEs in Denmark are presented in Table 2 according to Denmark Statistics

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

2.2 Qualitative Component

The qualitative work will comprise three parts: focus groups, scenario-based simulations, and interviews.

Focus Groups: Focus groups will be conducted with stakeholders, including SME executives, industry representatives, and policymakers. The goal is to understand the challenges and mental models associated with cybersecurity practices in Denmark. Focus groups are particularly useful for uncovering the opinions and understanding differences in perspectives among various groups [14].

Scenario-Based Simulations: Simulations will confront the participants with cybersecurity threats to test their responses and decision-making processes under stress. This method will help assess the practical applicability and robustness of policies in real-world scenarios [9].

Interviews: Follow-up interviews will be conducted with participants to gain deeper insights into individual and collective responses to the focus group sessions.

2.3 Target Groups

The study target three specific groups to which the qualitative component outlined above will be conducted with.

Policy Makers Level: This group includes top officials from national security and the Ministry of Foreign Affairs. They will participate in focus group workshops and scenario-based simulations to critically evaluate and map Denmark's cybersecurity strategies and policy-setting processes. The scenarios will be developed in collaboration with these policymakers to reflect their perceived threats and stress-test Danish companies accordingly.

Policy Promoters Level: Industry-level experts, such as officials from business associations, will participate in focus groups to complement the mapping from policymakers with their perspectives on the cybersecurity of business associations. Their input will also help refine the developed scenarios.

Policy Implementer Level: These are representatives from Danish SMEs. They will engage in structured simulations based on the developed scenarios to identify operational weaknesses and develop strategies that hinder responses to cyber threats. Focus group workshops with the representatives and further questionnaire surveys will complement the mapping of the Danish cybersecurity landscape with a company perspective.

2.4 Data Analysis

The study will utilize both statistical analysis for the survey data and thematic analysis as well as inductive coding for the qualitative data. This mixed-methods approach will enable a comprehensive mapping of the cybersecurity landscape, highlighting both quantitative trends and qualitative insights.

2.5 Limitations

The following limitations will likely apply to the research described before.

Limited Scope. The study focuses exclusively on Danish SMEs in the defense and IT sectors, which may not fully reflect the diverse cybersecurity landscapes across different industries or geographic regions.

Sample Size and Selection. The sample of 50 SMEs, while large enough for insightful results, may not capture the full variability of cybersecurity practices across the two sectors of defense and IT.

Bias. Focus group participants tend to intellectualize [14]. Additionally, we might encounter social desirability bias in the group discussions and survey responses.

Simulated Scenarios. While scenario-based simulations provide valuable insights into decision-making processes, they cannot perfectly replicate the complexities and unpredictability of real-world cyber threats, possibly limiting the applicability of the findings [10].

Methodological Constraints. The study's mixed-methods approach, although robust, faces the challenge of integrating qualitative and quantitative data, which may lead to inconsistencies.

2.6 Expected Contributions

The research is expected to reveal gaps between current cybersecurity policies and their impact and implementation in practice. The focus on mental models and stakeholder perspectives will provide a deeper understanding of the barriers to effective cybersecurity practices and help in formulating more targeted and practical policy recommendations.

3 Conclusion and Future Work

This study aims to map the Danish cybersecurity landscape from three perspectives, policymakers, business associations, and companies. Thereby, it highlights the unique vulnerabilities of Danish SMEs in critical sectors but also aims to derive concrete, actionable recommendations to enhance Danish cybersecurity defenses. The integration of scenario-based simulations with traditional survey methods provides novel insights into the effective alignment of cybersecurity policies with operational realities.

Further Research. In case the research outlined in this extended abstract yields the expected results, it might prove worthwhile to widen the scope to test the applicability of our findings across different sectors and countries.

References

[1] Virginia Braun and Victoria Clarke. *Thematic analysis.* American Psychological Association, 2012.

[2] Verizon Business. *2023 Data Breach Investigations Report (DBIR)*. Accessed: 2024-04-23. Verizon Business. URL: https://www.verizon.com/business/resources/T4b6/reports/2023-data-breach-investigations-report-dbir.pdf.

[3] CBS Wire. *Small and Medium-Sized Businesses Make Up 99 Percent of Denmark's Businesses but Are Hardly Represented at Universities*. Accessed: 2024-04-09. CBS Wire. URL: https://cbswire.dk/small-and-medium-sized-businesses-make-up-99-percent-of-denmarks-businesses-but-are-hardly-represented-at-universities/.

[4] Centre for Cyber Security (CFCS). *Cyber-threat Against Denmark 2023*. [PDF file]. Danish Defence Intelligence Service, 2023. URL: https://cfcs.dk.

[5] Dansk Industri. *SMVer er Danmarks vækstlokomotiver*. Danish. Accessed: 2024-04-03. Dansk Industri. URL: https://www.danskindustri.dk/di-business/arkiv/nyheder/2019/2/smver-er-danmarks-vakstlokomotiver/.

[6] W Alex Edmonds and Thomas D Kennedy. *An applied guide to research designs: Quantitative, qualitative, and mixed methods*. Sage Publications, 2016.

[7] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*. Tech. rep. Accessed: 2024-04-23. Oct. 2023. DOI: 10.2824/782573.

[8] European Union Agency for Cybersecurity (ENISA). *EU Cybersecurity Act and its Implications for SMEs*. Accessed: 2024-04-10. 2019. URL: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity.

[9] Rosemary Garris, Robert Ahlers, and James E Driskell. "Games, motivation, and learning: A research and practice model". In: *Simulation & gaming* 33.4 (2002), pp. 441–467.

[10] Margaret E Gredler. "Designing and evaluating games and simulations: A process approach". In: *(No Title)* (1992).

[11] IBM. *IBM Report: Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches*. 2024. URL: https://newsroom.ibm.com/2024-02-21-IBM-Report-Identity-Comes-Under-Attack,-Straining-Enterprises-Recovery-Time-from-Breaches (visited on 04/23/2024).

[12] IBM. *IBM X-Force Threat Intelligence Index 2024*. Accessed: 2024-04-23. 2024. URL: https://www.ibm.com/reports/threat-intelligence.

[13] IT University of Copenhagen and University of Southern Denmark. *Assessment on the Status of Cybersecurity in Denmark: Final Report*. Tech. rep. Accessed: 2024-04-09. Danish Centre for Cybersecurity, 2020. URL: https://ascd.dk.

[14] Richard A. Krueger and Mary Anne Casey. *Focus Groups: A Practical Guide for Applied Research*. 5th ed. Thousand Oaks, California: SAGE Publications, Inc, 2015.

[15] Organisation for Economic Co-operation and Development. *OECD Economic Surveys: Denmark 2024*. Accessed: 2024-04-03. Organisation for Economic Co-operation and Development. URL: https://fm.dk/media/27397/oecd-economic-surveys-denmark-2024.pdf.

[16] Organisation for Economic Co-operation and Development. *OECD iLibrary*. Accessed: 2024-04-03. Organisation for Economic Co-operation and Development. URL: https://www.oecd-ilibrary.org/sites/21687e3f-en/index.html?itemId=/content/component/21687e3f-en.

[17] Small Business Standards (SBS). *EU Cybersecurity Act and the Role of Standards for SMEs*. Accessed: 2024-04-23. 2020. URL: https://www.sbs-sme.eu/sites/default/files/publications/23032020%20SBS%20Position%20Paper_EU%20Cybersecurity%20Act%20and%20the%20role%20of%20standards%20for%20SMEs.pdf.

[18] *SMESEC*. https://www.smesec.eu/index.html. Accessed: 2024-04-23.

[19] Jan Stentoft and Ole Stegmann Mikkelsen. "The COVID-19 Pandemic has Increased the Awareness of Supply Chain Resilience, But Recovery Plans are Still Absent". In: *DILF Aktuelt* 7 (2020), pp. 47–54. URL: https://portal.findresearcher.sdu.dk/en/publications/4e0f5cdf-664c-4d03-841f-ec36d56c7826.

[20] The Danish Government. *Danish Cyber and Information Security Strategy 2022-2024*. Tech. rep. Accessed: 2024-04-09. Ministry of Finance, 2021. URL: https://fm.dk.

[21] David R Thomas. "A general inductive approach for qualitative data analysis". In: (2003).

[22] U.S. Securities and Exchange Commission. *Cybersecurity Challenges Facing Small and Midsize Businesses*. Accessed: 2024-04-23. U.S. Securities and Exchange Commission. URL: https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses.

4 Tables

Article 1 An enterprise is considered to be any entity engaged in an economic activity, irrespective of its legal form. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity.

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 which employ fewer than 250 persons and which 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 which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

Company Category	Staff Headcount	Turnover or	Balance Sheet Total
Medium-sized	<250	€50m	€ 43m
Small	<50	€ 10m	€ 10m
Micro	<10	€ 2m	€ 2m

Table 1: SME defined in EU Recommendation 2003/361

Firm Size (employees)	% of Firms	% of full time employees
SMEs (1-99)	98.7	38.7
Micro (1-9)	86.3	14.3
Small (10-49)	10.9	17.0
Medium (50-99)	1.4	7.4
Large (100+)	1.3	61.3

Table 2: Distribution of firms and employees, 2021
source: Danmarks Statistik