

THE IMPACT OF GENDER EQUALITY IN THE CYBERSECURITY SECTOR

RAGNHILD SOFIE ERTZEID TOFT
TUVA CECILIE EIKAAS

SUPERVISORS

Jaziar Radianti
Terje Gjøsæter

University of Agder, 2023
Faculty of Social Science
Department of Information Systems

Master

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

| | | |
|----|--|-----|
| 1. | Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen. | Ja |
| 2. | Vi erklærer videre at denne besvarelsen: <ul style="list-style-type: none">• Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands.• Ikke refererer til andres arbeid uten at det er oppgitt.• Ikke refererer til eget tidligere arbeid uten at det er oppgitt.• Har alle referansene oppgitt i litteraturlisten.• Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse. | Ja |
| 3. | Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31. | Ja |
| 4. | Vi er kjent med at alle innleverte oppgaver kan bli plagiattkontrollert. | Ja |
| 5. | Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk. | Ja |
| 6. | Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider. | Ja |
| 7. | Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet. | Nei |

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).

Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

| | |
|---|-----|
| Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering: | Ja |
| Er oppgaven båndlagt (konfidensiell)? | Nei |
| Er oppgaven unntatt offentlighet? | Nei |

Acknowledgements

First and foremost, we would like to express our gratitude to Professor Jaziar Radianti and Associate Professor Terje Gjørseter of the Department of Information Systems at the University of Agder for serving as our thesis advisers. Our meetings every other week have balanced our progress toward completing this thesis paper. Your tenacity and patience with us are commendable, and we sincerely value your efforts. Thank you for everything; we couldn't have done it without you!

Additionally, we'd also want to express our gratitude to the anonymous respondents who took the time to engage in this study and for their knowledge and insight, which contributed to the empirical evidence that enabled the master's thesis to be completed. A big thank you!

Last but not least, we would like to acknowledge and thank our parents. Your encouragement and support have been invaluable, given us the motivation to keep going. Without them, this endeavor would not have been feasible. Thank you!

Kristiansand,
June 1st, 2023



Tuva Cecilie Eikaas



Ragnhild Sofie Ertzeid Toft

Abstract

Nowadays, there is a shortage of cybersecurity professionals in the sector and women are disproportionately underrepresented in the field. This exploratory study examines how organizations can retain and entice women in the cybersecurity industry, as well as how enhanced gender balance affects the work environment. Because the scope is limited, we will only look at gender equality between men and women, as well as apply the study in a Norwegian context. Furthermore, the study investigates why women are underrepresented in cybersecurity and identifies barriers preventing them from pursuing this career. The findings of our systematic literature review (SLR) identifies obstacles and already existing solutions for increasing the representation of female cybersecurity professionals. To gain a comprehensive understanding of respondents' experiences with gender equality and diversity in the industry, qualitative research using semi-structured interviews (SSI) was conducted. Our study contains fourteen respondents from organizations with cybersecurity from both private and public sectors, with varying positions. The primary metric that emerged from both the interviews and the literature was showing possibilities of cybersecurity and raising awareness of the subject. By analyzing our literature- and empirical findings we demonstrated that there is a correlation between the barriers preventing women from cybersecurity. According to our theory, stereotypes, disinformation, discrimination, lack of role models and lack of knowledge about the cybersecurity contributes to low self-efficacy, which causes low interest in the subject, which leads back to the first point. By understanding how this is connected, we were able to propose several recommendations to reduce the barriers and turn the vicious cycle into a virtuous one. Based on our results, we developed a list of recommendations for enticing and retaining more women in cybersecurity, which can be applied in both educational and organizational sector.

The study's primary purpose is to help advance gender equality in the cybersecurity industry by identifying the barriers that keep women out of the field and providing long-term solutions for enticing and retaining more women. The recommendations are applicable to organizations outside of the cybersecurity industry as well, and this research can thus be applied to a variety of male-dominated sectors.

Keywords: Cybersecurity, gender equality, women, STEM

Contents

| | |
|---|------------|
| Acknowledgements | ii |
| Abstract | iii |
| List of Figures | vi |
| List of Tables | vii |
| List of Abbreviations | vii |
| 1 Introduction | 1 |
| 1.1 Rationale and Motivation | 2 |
| 1.2 Research Questions and Research Aims | 2 |
| 1.3 Research Approach | 2 |
| 1.4 Research Scope | 3 |
| 1.5 Research Overview | 3 |
| 2 Background and Related Work | 4 |
| 2.1 Literature Review | 4 |
| 2.1.1 Method | 4 |
| 2.1.2 Literature Criteria | 5 |
| 2.1.3 Search Process | 6 |
| 2.1.4 Screening | 7 |
| 2.2 Definition of Terms | 12 |
| 2.3 Possible Barriers of the Problem Statement | 13 |
| 2.3.1 Self-efficacy, Interest and Characteristics | 13 |
| 2.3.2 Stereotypes, Perceptions and Discrimination | 14 |
| 2.3.3 Career Opportunities | 16 |
| 2.3.4 The Impact of Role Models and Key Influencers | 17 |
| 2.4 Existing Measures | 17 |
| 2.5 What are the Effects of Gender Equality? | 18 |
| 2.6 Summary | 20 |
| 3 Research Approach | 21 |
| 3.1 Research Design | 21 |
| 3.2 Qualitative Approach | 23 |
| 3.3 The Unit of Analysis and Subject Selection | 24 |
| 3.4 Data Collection | 25 |
| 3.4.1 Interview Methodology | 26 |
| 3.5 Limitations of Interviews | 27 |
| 3.6 Data Analysis | 28 |
| 3.7 Ethical Considerations | 30 |

| | |
|---|-----------|
| 4 Empirical Findings | 31 |
| 4.1 Why Women are not in Cybersecurity | 32 |
| 4.1.1 Self-efficacy, Interest and Characteristics | 32 |
| 4.1.2 Stereotypes, Perceptions and Discrimination | 33 |
| 4.1.3 Career Opportunities | 34 |
| 4.1.4 The Impact of Role Models and Key Influencers | 35 |
| 4.2 How can the Cybersecurity Entice and Retain Woman? | 36 |
| 4.3 The Value of Female Participants in Organizations | 37 |
| 4.4 Summary | 39 |
| 5 Discussion | 40 |
| 5.1 Analysis of Findings | 40 |
| 5.1.1 Theoretical Implications of the Metric "Showing Possibilities" | 41 |
| 5.1.2 Implications for Practise | 43 |
| 5.1.3 The Effects of Female Cybersecurity Professionals in the Industry | 48 |
| 6 Conclusions | 49 |
| 6.1 Contribution to Theory and Industry | 49 |
| 6.2 Limitations and Future Directions | 50 |
| A Interview Guide | 52 |
| B Consent Form | 54 |
| Bibliography | 60 |

List of Figures

| | | |
|-----|---|----|
| 1.1 | Process map | 3 |
| 2.1 | The steps of systematic literature review (SLR). | 5 |
| 2.2 | Sustainable development goal 5 | 6 |
| 2.3 | Systematic literature review | 8 |
| 2.4 | Model of the impostor phenomenon by Neueiter and Traut-Mattausch | 14 |
| 2.5 | Organizational positions by gender globally | 15 |
| 2.6 | The correlation between a company’s financial performance and its level of diversity | 19 |
| 3.1 | A map of genres in qualitative research | 22 |
| 3.2 | Differences between quantitative and qualitative research methodologies . . . | 24 |
| 3.3 | The stages of semi-structured interview guide | 26 |
| 3.4 | NVivo data analysis | 29 |
| 4.1 | Proposed measures to entice and retain women in cybersecurity | 36 |
| 4.2 | The effects of gender equality in cybersecurity | 38 |
| 5.1 | The vicious cycle of not showing possibilities | 41 |
| 5.2 | The virtuous cycle of showing possibilities. | 43 |
| 5.3 | The recommendation’s overarching model | 47 |
| B.1 | NSD consent form | 54 |
| B.2 | NSD consent form | 55 |

List of Tables

| | | |
|-----|---|----|
| 2.1 | Must-have keywords | 7 |
| 2.2 | Could-have keywords | 7 |
| 2.3 | Reviewed articles | 11 |
| 3.1 | Subject selection | 25 |
| 3.2 | The various interview structures | 26 |
| 3.3 | Limitations and potential solutions with semi-structured interviews | 27 |
| 4.1 | Summary table of the interviewees | 31 |

| List of Abbreviations | |
|------------------------------|--|
| AIS | Journal of the Association for Information Systems |
| CS | Cyber Security |
| FBI | Federal Bureau of Investigation |
| ICT | Information and Communication Technology |
| IS | Information System |
| IT | Information Technology |
| MoSCoW | Must-have, Should-have, Could-have and and Will not have |
| NCSC | National Cyber Security Center |
| NSD | Norsk Senter for forskningsdata (Norwegian Center for Research Data) |
| NSF | National Science Foundation |
| RQ | Research Question |
| RSA | A conference named after "Rivest, Shamir and Adleman", a public-key cryptosystem |
| SCCT | Social Cognitive Career Theory |
| SLR | Systematic Literature Review |
| SRQ | Sub Research Question |
| SSI | Semi-Structured Interview |
| STEM | The areas of Science, Technology, Engineering and Mathematics |
| UNDIR | The United Nations Institute for Disarmament Research |

Chapter 1

Introduction

The significance of cybersecurity is increasing. There is no indication that this tendency will slow down as our society is more dependent on technology than ever before. Because of society's increasing reliance on computer technology, particularly the Internet, a "market" for specific computer-related crimes has emerged, and cyberthreat actors have evolved to become more intelligent, persistent, and coordinated than previously. According to the 2022 annual data breach report by the "Identity Theft Resource Center" the number of affected victims (422.1 million) increased by almost 41.5 percent from 2021 (Identity Theft, 2023). In terms of our ability to stop cybercrime in the future, the increase indicates a worrying trend. We are all susceptible to cybercrime, including small and large businesses, governmental and private organizations, technologically advanced people, and, of course, private individuals. As former FBI Director Robert Mueller famously stated, *"There are only two types of companies: those that have been hacked and those that will be"* (Fai and Goh, 2021). The former FBI director made this remark at the annual RSA conference in 2012, when the threat posed by cyberspace was mostly of interest to computer aficionados and geeks (Fai and Goh, 2021). Eleven years later, in 2023, cybersecurity is a shared responsibility that affects everyone (Fai and Goh, 2021). Threat actors are continuously on the search for loopholes or exploitable vulnerabilities and are willing to go to any length to uncover them. Neglecting cybersecurity might be extremely expensive and damaging, especially if personal or financial data were to be compromised.

Thus, developing cybersecurity knowledge is more crucial than ever and should be at the top of everyone's priority list. Particularly in light of the fact that there aren't enough professionals battling cybercrime nowadays. According to the (ISC)² Cybersecurity Workforce Study, they expects a global cybersecurity workforce of 4.7 million in 2022, representing an 11.1 percent increase over last year and 464,000 additional positions (ISC, 2022). Despite hiring over 464,000 new employees in the previous year, the cybersecurity workforce gap has expanded by more than twice as much as the workforce (ISC, 2022). Encouraging cybersecurity careers among young people is a step in the right direction that will assist to reduce the global skill gap in this industry. By addressing the gap between men and women, the skills shortfall may be overcome.

Given that women continue to be underrepresented in the cybersecurity profession, it will be crucially important to encourage more of them to pursue employment in this field. The IT industry has a long way to go compared to other industries, making this an exceptional instance worthy of its own study. According to a report by Cybersecurity Ventures, the gender gap in cybersecurity is even more pronounced, with women making up only 25 percent of the global workforce in 2022 (Ventures, 2022). This isn't because there aren't enough jobs available or qualified candidates; rather, women confront a variety of obstacles in this profession that keep them from pursuing this career. Despite the availability of many concepts and enrichment activities, no comprehensive solution that has a consistent and long-term

influence on females has been presented.

1.1 Rationale and Motivation

This study is significant since women continue to be notably underrepresented in the field of cybersecurity despite its increasing relevance. More women entering the field of cybersecurity not only helps to reduce the gender gap in the labor shortage, but it also broadens the pool of potential cybersecurity professionals and produces more creative solutions. To keep up with the always shifting threat landscape, one needs a broad skill set; this skill set cannot be adequately represented by a homogeneous group. Along with technical expertise, those in cybersecurity need to be able to communicate well, think critically, manage projects and coordinate well. When a variety of people with various talents are combined, the likelihood that the team will possess all these skills rises. This suggests that expanding the number of female cybersecurity professionals will benefit the industry greatly.

1.2 Research Questions and Research Aims

As a result, it is critical that we identify and address the barriers that prevent women from seeking professions in cyberspace in order to come up with methods to raise the participation rate in this field. This brings us to the research question we will try to answer:

- *RQ: "How can the cybersecurity industry entice and retain woman?"*

Additionally, to gain a comprehensive understanding of the topic and enable us to answer our research question, a sub research question is posed:

- *SRQ: "How might the increased representation of female cybersecurity professionals contribute to an organization?"*

The main objective of this study is to identify why few women are entering the cybersecurity industry and what may be done to raise the number. Based on the construction of a grounded theory from interviews with female cybersecurity professionals, the information gathered highlighted the elements that can influence decisions to enter and remain in the cybersecurity industry. The research's second objective is to offer academics and practitioners holistic view so they can create initiatives that will assist reduce gender inequality.

1.3 Research Approach

This study uses a qualitative research approach to examine and identify research gaps, as well as understanding women's experiences in the cybersecurity industry and the barriers that prohibit women from pursuing this profession. In this study, data is gathered mainly through semi-structured interviews and research publications from recognized journals. We developed a foundation of knowledge for the primary literature review of twenty-six publications with the purpose of generating an understanding of the barriers preventing females from participating in cybersecurity. For the interviews we chose a qualitative approach since it is intended to extract in-depth and detailed information. Thus, fourteen interviews were conducted between January and February 2023, lasting between forty and sixty minutes each, with respondents from seven organizations in Norway with a cybersecurity department. The theoretical foundation and empirical findings were provided by the systematic literature review and semi-structured interviews, enabling the research questions to be answered.

1.4 Research Scope

The intent of this study's scope was to give an in-depth knowledge of the issue of women's underrepresentation in the cybersecurity industry. The problem, however, isn't that there are too many males working in the field; rather, it's that there aren't enough women. We intended to focus on women's perspective because they are the minority in cybersecurity, and we wanted to understand their reasoning for the challenges of a career in this industry. As a result, our study focused solely on the female perspective since we sought input from those who are directly connected to the barriers that limit greater participation of women in cybersecurity. In the research, there was no comparison between the experiences of male and female cybersecurity experts. The study maintained its emphasis on the experiences of women by omitting male cybersecurity experts.

1.5 Research Overview

Chapter 1 - Introduction - gives an overview of the study's research question and the problem statement.

Chapter 2 – Background and Related Work - outlines the process of doing a literature review as well as the background knowledge and relevant research that serve as the study's pillars.

Chapter 3 – Research Approach - provide justifications for why the selected research methodology and its underlying philosophical assumptions are appropriate for this research. Additionally, the research design, data gathering, interview methodology, interview limits, data analysis, validity, and ethical concerns are discussed.

Chapter 4 – Empirical Findings - in this section, we share the findings gathered from the interviews.

Chapter 5 – Discussion - we address here both our findings in relation to the research question and findings from other studies.

Chapter 6 – Conclusion - reaches a conclusion and briefly considers the contributions to theory and industry, as well as the research's limits and future directions.

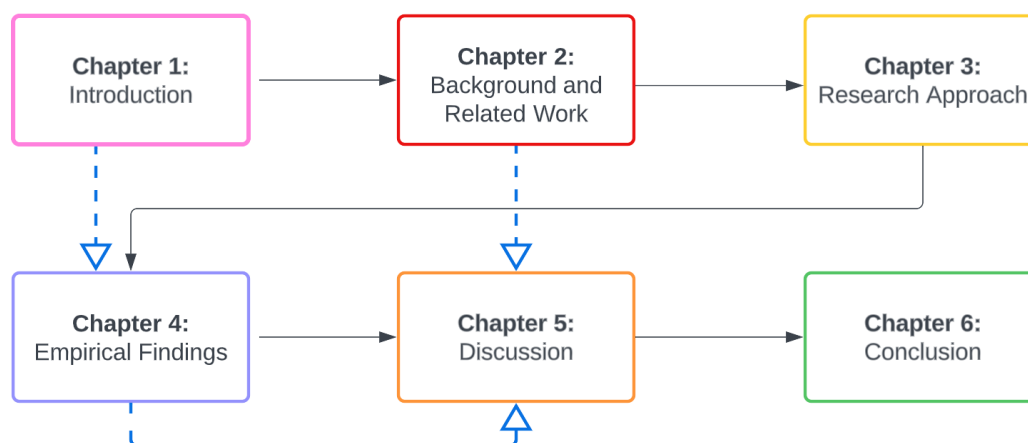


Figure 1.1: Process map

Chapter 2

Background and Related Work

In this chapter, we discuss the steps involved in conducting a literature review, such as the method selection, literature criteria, search, and screening procedures. Then, an overview of prior research thought to be pertinent to our study is provided, along with an explanation of how this literature influences the term project.

2.1 Literature Review

A literature review is a more or less systematic method of gathering and synthesizing prior research (Snyder, 2019). In this project, we used a systematic literature review (SLR) approach to select and discover research that supports the research question and helps us achieve our objectives. The main reason for conducting a systematic literature review was to gain a better understanding of how to propose a dynamic solution for attracting and retaining women in the cybersecurity industry. The rationale for conducting a systematic literature review is that it is a precise methodology that reduces the likelihood of biased results while also providing information about the effects of an aspect across a wide range of settings and empirical methods (Kitchenham and Charters, 2007). Furthermore, using this method may help to identify areas that require additional research to fill gaps in our knowledge. It has the potential to draw attention to methodological issues in research projects, which will aid future work in the field. Finally, it can be used to determine which questions have obvious answers based on the facts available and do not necessitate further investigation.

2.1.1 Method

An initial systematic literature review was performed previously to provide a solid foundation for this thesis. At this point, a screening was performed to identify relevant literature, followed by another screening before using the "snowball method" from these articles to shape the new literature review. The snowball approach involves tracking down references from other texts and articles, and it is a strategy of locating literature that begins with a key document on your topic. Furthermore, we chose to conduct a systematic literature review to identify research that is most beneficial to the thesis. Although there are many advantages to using a systematic literature review approach, one major disadvantage is the amount of time and effort required in comparison to traditional literature reviews. Figure 2.1 depicts the three key processes that must be included for a successful review: planning, conducting, and reporting (Xiao and Watson, 2019).

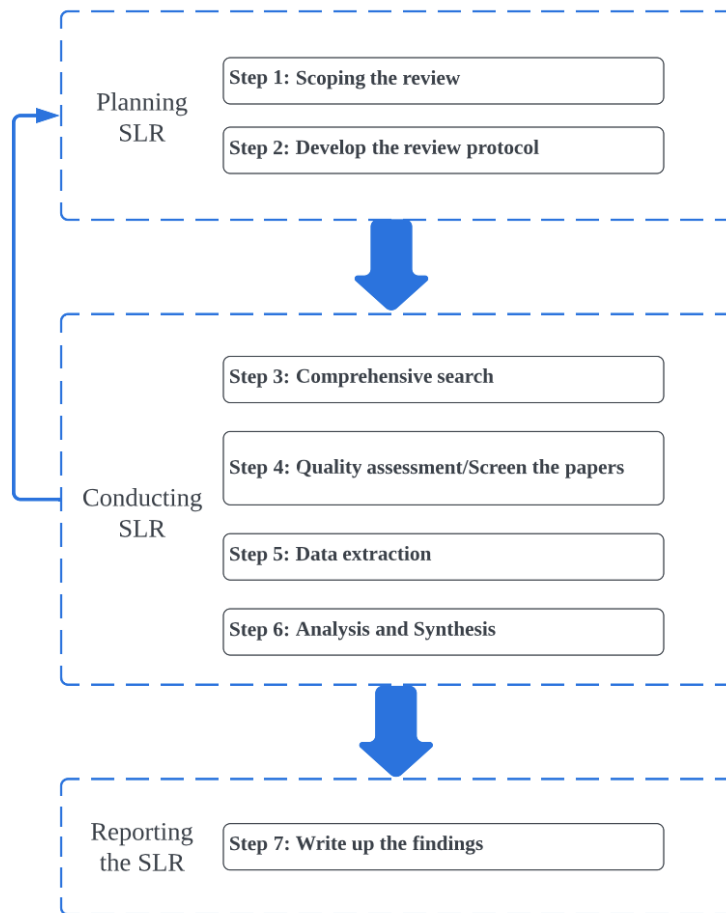


Figure 2.1: The steps of systematic literature review (SLR).
(Chompunuch et al., 2019)

2.1.2 Literature Criteria

Criteria for related research must be established in order to help gather results that are more closely related to the research problem. The procedure includes criteria for selection, search approach, data collection, data display, analysis, and synthesis.

- The articles must be written in either English or Norwegian.
- The articles must include a keyword combination related to our research problem.
- The articles must be sourced from reputable sources and be found in our chosen databases.
- To remain relevant, the articles should be no more than 9 years old, given that sustainable development, which includes gender equality, did not become a global goal until 2015 (Women, 2022). The deadline for achieving gender equality and the empowerment of all women and girls is 2030 (Women, 2022). Figure 2.2 depicts the critical need to increase commitment to this goal; otherwise, gender equality will remain an unrealized goal.

Note: Keep in mind that publications on topics other than technology or gender equality may be older.

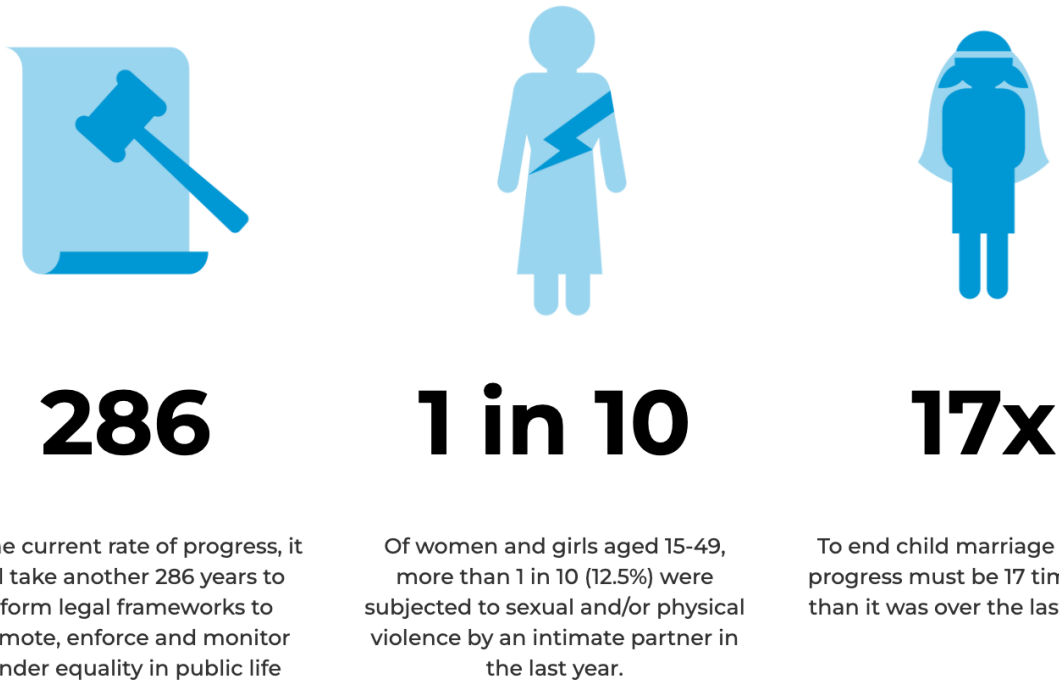


Figure 2.2: Sustainable development goal 5 (Women, 2022)

2.1.3 Search Process

The systematic search for literature is recognized as an important component of the systematic review process because it identifies material for the review. It includes a methodical search for studies and aims to provide readers with a clear summary of study identification, demonstrating how studies were discovered and how the review results fit into the relevant evidence (Cooper et al., 2018). When looking for relevant literature, electronic databases have been the primary source. These databases are the main source of published literature collections (Patticrew and Roberts, 2006). As a result, during the literature review process, the databases JSTOR, AIS eLibrary, Scopus, ProQuest, and the search engine Google Scholar, were used to search for relevant literature. These search engines provide sufficient results for our purposes because they collect literature from various sources and provide an extensive library of content.

To find relevant literature, we created a set of key-words that were used in developing the search strings. In addition, aspects of the MoSCoW method are in use. This is a search strategy that aids in the prioritization of searches, and stands for must have, should have, could have, and will not have (Khan et al., 2015). By categorizing keywords as Must-have and Could-have, we can still include keywords that may provide valuable publications without risking over flooding the search with irrelevant material. As a result, articles used in this literature review must include the Must-have keywords shown in Table 2.1, but not necessarily the Could-have keywords viewed in Table 2.2. An overview of the selected keywords in English is provided below. In the search phrase, BOOLEAN operators such as "AND" and "OR" are used to alternate between must-have and could-have keywords.

Must-have keywords:

| Keywords | Synonym / Abbreviation |
|-----------------|--|
| Cybersecurity | Cyber security Cyber defence Information security Network security Cyber |
| Gender equality | Gender diversity Equal opportunities Gender non-discrimination Gender balance Gender equity Diversity |
| Sector | Industry Organization Area Field Enterprises Business |
| Women | Female Girl |

Table 2.1: Must-have keywords

Could-have keywords:

| Keywords | Synonym / Abbreviation |
|--------------------|--|
| IT | Information technology Computer technology Computer science STEM ICT |
| Gender differences | Gender inequality Gender bias Gender disparity Gender discrimination Gender inequity Gender gap |

Table 2.2: Could-have keywords

2.1.4 Screening

The screening approach was used after compiling a list of references to determine whether publications should be included for data extraction and analysis. (Xiao and Watson, 2019). Following the compilation of the reference list from the initial and supplementary searches, we conducted a screening process to include and exclude literature in accordance with the established selection protocol and article criteria. Figure 2.3 depicts a PRISMA flow diagram to help visualize the process.

The process began by compiling a list of references from database searches. 54 articles remained after looking through the identified articles and deleting duplicates. Any publications with irrelevant titles that had no relevance to the study were excluded. Furthermore, the remaining 32 publications were evaluated based on their abstracts to determine their relevance. We were left with 21 articles after screening the abstracts. Following that, the articles were analyzed using full-text screening. This entailed assessing the most relevant material from each publication, such as summaries, findings, results, and conclusions, as well as analyzing the quality of the works. As a result, nine of the articles were removed. We finished the procedure by snowballing from the 12 appropriate papers identified, and the final screening process resulted in 26 articles.

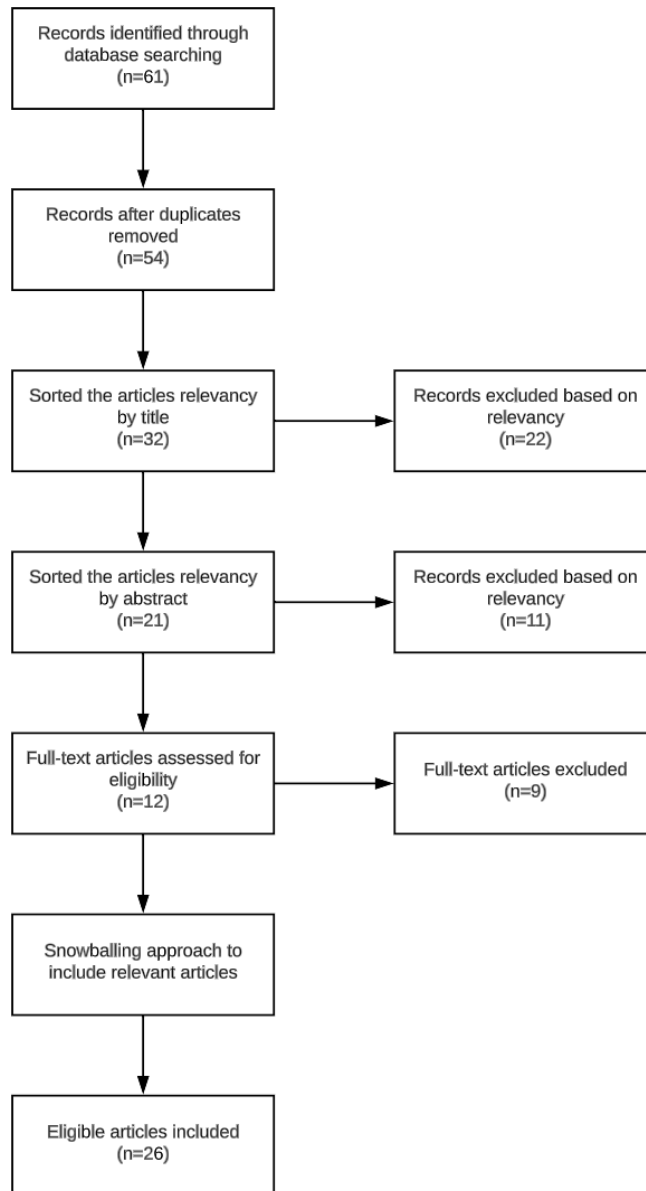


Figure 2.3: Systematic literature review

Table 2.3 displays the 26 qualified and chosen articles from the screening process.

| Author (Year) | Source | Title | Keywords |
|---|--|---|--|
| Cedric Herring, (2017) | American Sociological Review: | Is Diversity still a good thing? | Gender diversity |
| Matthew Gouett, (2021) | International Institute of Sustainable Development: | Furthering Gender Equality Through Gender bonds | Gender inequality, Gender equality, Gender diversity |
| Donna Peacock & Alastair Irons, (2017) | International Journal of Gender, Science and Technology: | Gender Inequalities in Cybersecurity: Exploring the Gender in Opportunities and Progression | Cybersecurity, Gender inequality, Gender equality, Women, Sector |
| Zacharias C. Zacharia et al., (2020) | European Parliamentary Research Service: | Education and employment of women in science, technology and the digital economy, including AI and its influence on gender equality | Cybersecurity, Gender inequality, Gender equality, Women, Sector |
| Elizabeth Weingarten & Megan E. Garcia, (2015) | New America: | Decrypting Cybersecurity's Gender Gap | Cybersecurity, Gender equality, Industry, Women |
| Pam Rowland, et al., (2018) | AIS Journals: | CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path | Cybersecurity, Gender gap, Girls, Sector, Gender diversity |
| Kembley Kay Lingelbach (2018) | Nova Southeastern University: | Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field | Cybersecurity, Gender equality, Female, Field |
| Carrie L. Pifer (2017) | Frostberg State University: | Cybersecurity Workforce Alert: Women's Perspectives on Factors Influencing Female Interest | Female, Cybersecurity, Field, Gender equity |
| Sapna Cheryan, Allison Master & Andrew N. Meltzoff (2015) | University of Washington: | Cultural stereotypes as gatekeepers: increasing girls' interest in computer science and engineering by diversifying stereotypes | STEM, Gender equality, Girls |
| Justin Scott Giboney, et al., (2018) | Association for Educational Communications & Technology: | Increasing Cybersecurity Career Interest through Playable Case Studies | Cybersecurity, STEM, Sector, |

| Author (Year) | Source | Title | Keywords |
|--|---|--|---|
| Kaspersky (2018) | Kaspersky Lab | Beyond 11%: A study into why women is not entering cybersecurity | Cybersecurity, Gender gap, Gender equality, Women, Sector |
| (ISC)2 (2022) | (ISC)2 | (ISC)2 Cybersecurity Workforce Study 2022 | Cybersecurity, Gender gap, Organization |
| Chris Sakellariou & Zheng Fang (2021) | International Journal of Educational Research | Self-efficacy and interest in STEM subjects as predictors of the STEM gender gap in the US: The role of unobserved heterogeneity | STEM, Gender gap |
| Una Tellhed, Martin Bäckström & Fredrik Björklund (2017) | Sex Roles | Will I Fit in and Do Well? The Importance of Social Belongingness and Self-Efficacy for Explaining Gender Differences in Interest in STEM and HEED Majors | Gender differences, STEM, Girls |
| Randolph C. H. Chan (2022) | IJ STEM Ed | A social cognitive perspective on gender disparities in self-efficacy, interest, and aspirations in science, technology, engineering, and mathematics (STEM): the influence of cultural and gender norms | STEM, Gender norms |
| Ming-Te Wang & Jessica L. Degol (2017) | Educ Psychol Rev | Gender Gap in Science, Technology, Engineering, and Mathematics (STEM): Current Knowledge, Implications for Practice, Policy, and Future Directions | Gender gap, STEM, |
| Laura Amo (2016) | IEEE | Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy | Gender gap, Cybersecurity, Women, gender equality, Sector |
| Adel Ismail Al-Alawi (2023) | Journal of International Women's Studies | Women in Cybersecurity: A Study of the Digital Banking Sector in Bahrain | Cybersecurity, Women, Sector, |
| Sebastian Lihammer & Linnea Hagman (2021) | KTH Royal institute of technology | Investigating Gender Disparity within Cyber Security | Cybersecurity, Gender disparity, Sector, Women, Gender equality |
| Michelle Johnson Cobb (2018) | Computer Fraud & Security | Plugging the skills gap: the vital role that women should play in cyber-security | Cybersecurity, Women, Gender diversity, Business |

| Author (Year) | Source | Title | Keywords |
|---|-------------------------------|---|--|
| Frost & Sullivan (2017) | (ISC)2 | The 2017 Global Information Security Workforce Study: Women in Cybersecurity | Cybersecurity, Women, Organization, Gender diversity |
| Swagata Das (2020) | University of Georgia | Conceptualizing the Experiences of Women's Career Development in Cybersecurity: A Narrative Study | Cybersecurity, Women, Field, Gender diversity |
| Vivian Hunt et al., (2015) | McKinsey& Company | Diversity matters | Gender diversity |
| Letian Zhang et al. (2019) | Harvard business review | Research: When gender diversity makes firms more productive | Gender diversity |
| Aina E. Olaiya and Cameron A. Patronella (2011) | Dimensions of Early Childhood | Why Does Gender Matter? Counteracting Stereotypes With Young Children | Gender equality |
| Carl Willis-Ford (2018) | University of Fairfax | The perceived impact of barriers to retention on women in cybersecurity | Cybersecurity, Women, Industry, Gender diversity |

Table 2.3: Reviewed articles

2.2 Definition of Terms

Some words must be defined and clarified in order to achieve a consistent understanding of essential concepts and terms utilized in this study. Gender equality, gender diversity, gender balance, cybersecurity and cybersecurity professionals are some of the phrases used. It is especially important to define the first two concepts because they are frequently confused with one another.

- **Gender equality:** For the purposes of this study, we have decided to use the UN's definition of gender equality. Gender equality refers to women and men, as well as girls and boys, having equal rights, responsibilities, and opportunities (Women, n.d.). Equality does not imply that men and women will become identical, but rather that men and women's rights, responsibilities, and opportunities will not be determined by whether they are born male or female (Women, n.d.). The concept of gender equality indicates that the interests, needs, and goals of both men and women are taken into account, while also acknowledging the diversity of varied groups of women and men (Women, n.d.).
- **Gender diversity:** We chose the Skills 4 definition for this study because they are an award-winning diversity and inclusion training provider in STEM. Gender diversity is simply the equal representation of men and women (Skills4, 2023). Gender diversity in the workplace, more specifically, means that women and men are hired at a similar and consistent rate, are paid equally, and are given the same opportunities, whether it is access to resources, promotions, or pay (Skills4, 2023).
- **Gender balance:** According to UNICEF, gender balance refers to; a human resource issue requiring equal involvement of men and women in all areas of work (international and national personnel at all levels, including senior positions) and initiatives initiated or supported by agencies (UNICEF, 2017).
- **Cybersecurity:** The National Cyber Security Center (NCSC) defines cybersecurity as the process by which individuals and organizations reduce the danger of a cyber attack (National Cyber Security Center, n.d.). The primary goal of cybersecurity is to secure the devices we all use (smartphones, laptops, tablets, and computers), as well as the services we use - both online and at work - from theft or damage (National Cyber Security Center, n.d.). Cybersecurity is also about preventing unauthorized access to the massive amounts of personal information we preserve on these devices and online (National Cyber Security Center, n.d.).
- **STEM:** According to the U.S. Department of Education, STEM is an acronym for science, technology, engineering, and math (U.S. Department of Education, 2021). These four sectors, which emphasize innovation, problem solving, and critical thinking, are required for countries to build their economies and remain globally competitive (U.S. Department of Education, 2021).
- **Cybersecurity professionals:** A cybersecurity professional is a specialist and expert in the field of information technology security (Simplilearn, 2023). They are in charge of safeguarding the IT infrastructure, edge devices, networks, and data (Simplilearn, 2023). A cybersecurity expert is specifically responsible for preventing data breaches and responding to assaults (Simplilearn, 2023).

2.3 Possible Barriers of the Problem Statement

For women to fully engage in cybersecurity, barriers to entry, retention, and growth must be mitigated. We will thus briefly review some of the barriers that the literature identifies as preventing women from entering the profession or from succeeding in computer science and cybersecurity fields before moving on to some interesting current solutions to the barriers and finally looking at the effects of gender equality.

2.3.1 Self-efficacy, Interest and Characteristics

The STEM gender gap is acknowledged to be significantly influenced by gender disparities in ability beliefs, notably self-efficacy (Sakellariou and Fang, 2021). Self-efficacy can be superficially explained as the conviction that one can succeed in a particular field (Tellhed et al., 2017). According to the Social Cognitive Career Theory (SCCT), the development of interests and future educational and vocational choices are significantly influenced by self-efficacy, or perceived skills to learn or perform well in a certain sector (Chan, 2022). Researchers have discovered that self-efficacy is one of the most important factors in effectively completing computer activities, implying that self-confidence is crucial for a cybersecurity professional (Lingelbach, 2018). It appears that women tend to have substantially poorer self-efficacy in computer science and cybersecurity in particular, which is one reason why they may decide against pursuing studies and professions in these sectors. Males, on the other hand, frequently think they are equally capable of handling occupations that are dominated by men and women (Tellhed et al., 2017). As seen by research, males often apply if they believe they fulfill 60% of the stated qualifications, but women typically apply when they believe they match 100% of the requirements, creating a candidate pool that is overwhelmingly male (Cobb, 2018). According to Cheryan, Master and Meltzoff one of the reasons why women may decide against pursuing cybersecurity is that girls systematically underestimate themselves in how well they will do in these fields, and this predicts their lower interest in entering them (Cheryan et al., 2015). A research from the European Parliament's Policy Department for Citizens' Rights and Constitutional supports the argument that a woman's self-efficacy appears to be one of the biggest personal barriers (Zacharia et al., 2020). This is justified by the fact that women do not choose this field as a profession since they have poorer self-efficacy when it comes to data/IT skills (Zacharia et al., 2020).

In a five-day cybersecurity camp for teens, Laura Amo analyzes gender disparities in the self-efficacy and interest of cybersecurity. According to the study's findings, boys initially outperformed girls on the Cybersecurity Engagement and Self-Efficacy Scale, with considerably stronger involvement and self-efficacy in cybersecurity (Amo, 2016). The disparity in cybersecurity engagement and self-efficacy ratings between boys and girls, however, vanished by the end of the week (Amo, 2016). As a result of the workshops, the girls students caught up to their male colleagues, demonstrating how such experiences might close the gender gap in cybersecurity engagement and self-efficacy (Amo, 2016).

Knowing the importance of self-efficacy in the decision-making process and career pursuit, it is extremely alarming that women have much lower self-efficacy scores than men do in computer science, and cybersecurity in specific. Particularly given that past study has revealed that girls and boys score equally well in academics, but that parents and teachers frequently underestimate females' mathematical ability and believe that boys will succeed better than girls in the STEM fields (Chan, 2022). Children's perceptions of their skills and parents' gender prejudices are frequently related (Chan, 2022). This idea is supported by Wang and Degol, who discovered that if their parents display greater levels of gender prejudice, girls are more likely to perceive they lack competency in STEM subjects, even while they outperform males in STEM, and that this may, in turn, impair self-efficacy in STEM among girls (Wang

and Degol, 2017). Internalized gender roles and their effects on self-efficacy may lead girls to believe they are unsuited for STEM, which discourages them from pursuing STEM-related careers (Chan, 2022).

The model below in Figure 2.4, developed by Neueiter and Traut-Mattausch, neatly depicts how self-efficacy, or "imposter syndrome" in this context, affects one's career (Willis-Ford, 2018). Imposter syndrome can be roughly defined as having doubts about what you're capable of. Studies demonstrate that males are less likely than women to experience the impostor phenomenon, and even when they do, it typically occurs in a milder form (Willis-Ford, 2018).

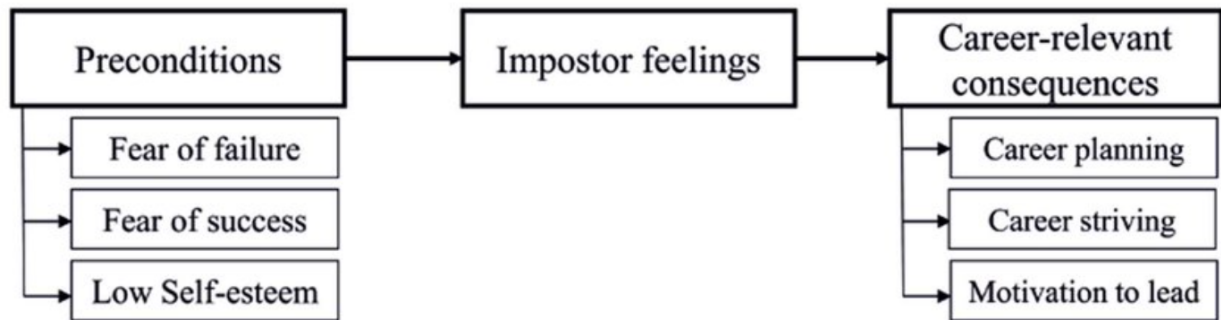


Figure 2.4: Model of the impostor phenomenon by Neueiter and Traut-Mattausch (Willis-Ford, 2018)

This is related to the fact that women have a hard time visualizing themselves working in the field of cybersecurity because they feel they lack the necessary abilities. According to some respondents in a research by Johnson, males were perceived as being more competitive and drawn to the notions of "attack" and "defend," and that the majority of the field's characteristics were intended to appeal to them (Willis-Ford, 2018). Due to the fact that employers nowadays aren't only seeking for coders, the problem here is one of awareness (Kaspersky, 2018). Although problem-solving and critical thinking abilities are equally important for a career in cybersecurity, the outsider's perspective on the field tends to concentrate mostly on the technical aspects (Kaspersky, 2018). It's important to let women know they don't need to be skilled coders to succeed in the field of cybersecurity. There are many other abilities that would be desirable to prospective employers and all of them would contribute to closing the present skills gap (Kaspersky, 2018).

2.3.2 Stereotypes, Perceptions and Discrimination

The research on this issue emphasizes how stereotypes and disinformation about the cybersecurity profession are among the barriers contributing to the gender discrepancy, and how critical it is to dispel these myths. According to Weingarten and Garcia negative stereotypes and lack of knowledge about what cybersecurity is and who is qualified to work in the field are some of the main causes of this gender gap (Weingarten and Garcia, 2015). They contend that the impression of cybersecurity experts as "young, white, basement-dwelling, and hooded men who break into computers" is widespread in the industry and that this perception might be a significant barrier for young women considering careers in the field (Weingarten and Garcia, 2015). Weingarten and Garcia's claims are supported by a study by Peacock and Irons, whose findings indicate that respondents believe that data security is perceived as a "man's job" by the general public as well as by customers and clients (Peacock and Irons, 2017). Al-Alawi, Al-Khaja, and Mehrotra add that most persons preoccupied with information technology are labeled "nerds" because they enjoy working with

complex IT systems, and these attributes are stereotypically given to men rather than women (Al-Alawi et al., 2023). Furthermore, stereotypes that portray computer scientists as being more technologically inclined than people-oriented or even deficient in interpersonal skills, in contrast to the assumption that women should be socially adept and people-oriented, act as a disincentive for women more so than for males (Lihammer and Hagman, 2021). This is a common misconception in the field, as many women are unaware that they do not need to be conventionally "technical" since all businesses want cybersecurity personnel, and cyber job is as much about the human component as it is about the technology (Weingarten and Garcia, 2015). Despite the fact that these views are wholly unrelated to reality, people's beliefs have a significant influence on their attitudes, behaviors, and decisions. Therefore, it is highly necessary to debunk these stereotypes as many women's perceptions of themselves or the image they strive to portray are incompatible with computer science norms, impacting their sense of belonging and driving them away (Lihammer and Hagman, 2021).

Although there is still more work to be done on the subject, research conducted by Aina E. Olaiya and Cameron A. Patronella discusses counteracting stereotypes with young children as a measure for confronting stereotypes. Children begin to form gender concepts around the age of two, and by the age of three, most children know whether they are a boy or a girl (Olaiya and Petronella, 2011). Children develop their gender identity and begin to understand what it means to be male and female between the ages of three and five (Olaiya and Petronella, 2011). Almost directly after becoming gender aware, children begin developing stereotypes, which they apply to themselves and others, in an attempt to give meaning to and gain understanding about their own identity (Olaiya and Petronella, 2011). The research of Aina E. Olaiya and Cameron A. Patronella demonstrates the importance of changing children's perception of gender roles to remove the traditional stereotypes of "male and female professions".

Due to widespread sexism, severe gender discrimination, and a lack of diversity, the technology industry continues to have difficulty recruiting, keeping, and progressing women (Das, 2020). Reed and her co-authors discovered that women face workplace discrimination, professional segregation, and income disparity in their study of women in cybersecurity (Frost and Sullivan, 2017). Despite women entering the cybersecurity industry with greater qualifications than males, they found that men are four times more likely than women to obtain C-level jobs (the top positions in organizations) as well as executive management roles and nine times more likelier to be in a managerial positions (Frost and Sullivan, 2017). Figure 2.5 illustrates this.

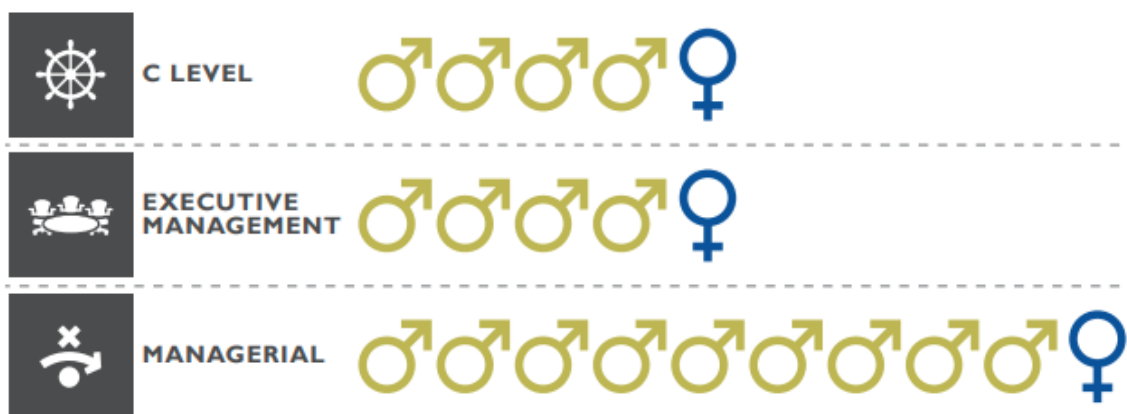


Figure 2.5: Organizational positions by gender globally (Frost and Sullivan, 2017)

Thankfully, attitudes towards gender discrimination and inequality are shifting. As a matter of fact, there was great public outrage when a Google employee published a blog claiming that women are inherently less suited for professions in technology (Cobb, 2018). Even if the response against this stereotype is heartening, the fact that this now-famous blog was ever published shows that not everyone in the workplace recognizes the benefits of diversity (Cobb, 2018).

2.3.3 Career Opportunities

Cybersecurity is one of the fastest growing career fields with qualified professionals in high demand growing at a rate 3.5 times faster than traditional information technology, and 12 times faster than the overall job market (Pifer, 2017). Women are significantly underrepresented in this industry (Peacock and Irons, 2017), despite the fact that organizations with greater gender diversity in their executive teams are 25% more likely to outperform organizations with less diversity (Gouett, 2021). Although accounting for nearly half of the global workforce, according to Cybersecurity Ventures women account for only 25% of cybersecurity professionals worldwide (Ventures, 2022). Several articles claim that cybersecurity and other STEM fields are still considered a "man's job," while other studies claim that the rate at which women leave this male-dominated workplace is precisely what contributes to the low rate of female entry (Peacock and Irons, 2017). Furthermore, Cheryan, Master, and Meltzoff believe that women are underrepresented not only because they leave the profession, but also because they are less likely to choose the field as a college major and career option (Cheryan et al., 2015). The fact that relatively few women choose this profession is a self-reinforcing effect that has a major impact as it discourages other women from following this career path. According to Kaspersky, young women are often unaware of cybersecurity as a career path or does not feel adequately prepared (Kaspersky, 2018). However, Leila Hoteit argues that the perception of women being less aware of cybersecurity to be false, as her survey found that 82% of the respondents had some or much knowledge of cybersecurity (Hoteit, 2022). The survey also discovered that women with low cybersecurity awareness have more negative perceptions of those who work in the field (Hoteit, 2022). These women believe the stereotypes of "hackers" to be true, whereas women who are more knowledgeable about cybersecurity have a more positive view of these workers (Hoteit, 2022). Furthermore, the survey investigated other barriers for women not pursuing a career in cybersecurity, with answers ranging from it being "a boy's club" to a lack of information, skill, and knowledge about cybersecurity, and finally, not being exposed to the field and having no role models (Hoteit, 2022).

According to Fortune Business Insights, the cybersecurity market is expected to grow from \$165.78 billion to \$366.10 billion between 2021 and 2028 (Insights, 2022), despite a global shortage of 3.4 million cybersecurity workers, according to the 2022 (ISC)² Cybersecurity Workforce Study (ISC, 2022). Because of the shortage, women will have unprecedented opportunities to advance to higher-level information security positions. Larger corporations are beginning to recognize that diverse teams can better identify and neutralize threats; "Anytime you can get diversity, you expand the overall perspective of a group." (Insights, 2022). Therefore, despite studies indicating that women are underrepresented in the cybersecurity field, the trend is gradually changing. The new trend can give women who are just starting out in the field an advantage in the job competitions.

2.3.4 The Impact of Role Models and Key Influencers

The lack of role models or key influencers is arguably the most important reason why women are underrepresented in cybersecurity. Without role models and others in the field to look up to and admire, women are all too likely to dismiss cybersecurity as a career option. Men are more likely than women to understand what the role entails, which is likely due to a lack of female role models in the industry (Kaspersky, 2018). However, 69% of young people have never met a cybersecurity professional, and only 11% have met a female cybersecurity professional (Kaspersky, 2018). And according to a Kaspersky survey, when they do meet someone working in cybersecurity, their perception of the role improves dramatically (Kaspersky, 2018). This demonstrates the importance of role models in highlighting the cybersecurity field as a whole, as well as how female personalities can be used to make cybersecurity more appealing to women and help to close the gender gap that exists today.

The lack of female role models is central to connecting the dots and changing perceptions at every stage of enticing and retaining women in cybersecurity. Organizations that want to attract the next generation of employees must be willing to seek out suitable internal representatives to help inspire young women (Kaspersky, 2018). This also applies to universities, where the low number of IT graduates means that there is an overrepresentation of males in teaching roles due to a much smaller group of people who are able to join the profession, resulting in a lack of positive female role models in education (Peacock and Irons, 2017). Other reasons for women not pursuing careers in technology include a lack of familial encouragement, which could be due to a lack of parental knowledge and/or confidence in technology, a lack of early engagement, a lack of encouragement within schools, a lack of appropriate careers education, as well as a lack of female role models (Peacock and Irons, 2017). These are all barriers which could impact on women's aspirations and awareness of opportunities in the industry. According to D'Hondt, it is clear that family encouragement and early exposure to technology are important factors in breaking down these barriers and bringing women into the cybersecurity field (Lingelbach, 2018). Parents and primary educators are critical in introducing cybersecurity and other STEM subjects to young girls to spark their interest. People, particularly women, prefer careers that are meaningful, have an impact on something important, and are engaging (Kaspersky, 2018). Cybersecurity jobs fits these criteria, one just need to improve how to communicate and educate this (Kaspersky, 2018).

2.4 Existing Measures

In addition to describing some of the barriers that prevent women from entering the field of cybersecurity, the literature also describes some existing measures to encourage more women to enter this field. Despite the fact that there is still a gender imbalance in cybersecurity, there are numerous initiatives aimed at increasing women's participation. Existing initiatives to address female underrepresentation in cybersecurity have had mixed results. However, in order to investigate new ideas and solutions for how to attract and retain more women in this field, it is critical to investigate existing proposals.

The literature emphasizes that gender disparity, as well as stereotypes, misconceptions, and a lack of encouragement or early engagement, are among the major causes of the gender gap in cybersecurity. Despite the fact that the literature stresses the importance of removing these barriers, only a few of them propose solutions. Rowland, Podhradsky, and Plucker propose the CybHER program as an alternative to other girl groups that support women in technology in order to reduce gender disparities in the field (Rowland et al., 2018). CybHER is an initiative to mentor and connect girls in cybersecurity (Rowland et al., 2018). Initiatives like this help to build not only a network, but also a community of women who

share common interests. CybHER and similar initiatives provides an anchor to the cybersecurity field by empowering, motivating, educating, and changing the perceptions of girls and women about cybersecurity (Rowland et al., 2018). This network, or community, helps women in cybersecurity feel less alone and is a measure to ensure women's retainment in the field.

Initiatives like CybHER are efficient at both providing a safe environment for women in cybersecurity and retaining women in the field. However, attracting more women to the field is equally important. Lingelbach's research discovered that there is a lack of awareness of cybersecurity, and that early exposure to technology and cybersecurity awareness, as well as knowledge and practice, can boost confidence and self-efficacy (Lingelbach, 2018). "Exposure," according to participant 2 in Lingelbach's study, is one way to entice women into cybersecurity (Lingelbach, 2018). "Early exposure, you know, from kindergarten on up, and introducing it more in schools. They do have those girl camps, but they do not have them here locally" (Lingelbach, 2018). Nearly all of her participants agreed on the importance of early education and exposure for attracting more women to cybersecurity. Several participants mention various educational programs for children and their effects, but they also mention a lack of accessibility to those programs and a scarcity of them. To attract a larger and more diverse student population to cybersecurity careers, interventions that leverage the strengths of competitions and camps while also overcoming some of their inherent limitations are required (Giboney et al., 2021). According to research, interventions that build confidence, use active learning, and assist students in identifying as a STEM professional are required to increase persistence in STEM majors such as cybersecurity (Giboney et al., 2021). By attracting more females into cybersecurity through early exposure, education and the development of self-efficacy, more will choose this career path. Hopefully this will result in the stereotypes of cybersecurity professionals to diminish, and thereby enticing even more women.

The literature established that both exposure and education are important measures in attracting women into cybersecurity. This can also be useful in correcting the misconceptions of cybersecurity and what it actually is. Weingarten and Garcia argue that a lack of knowledge about cybersecurity, are a reason for the gender gap (Weingarten and Garcia, 2015). Misconceptions about the field stem from a lack of knowledge, and it is not uncommon to believe that one must be extremely technically inclined to pursue such a career. As a result, emphasizing the human aspects of cybersecurity may be a good strategy for attracting more women to the field, as they are often looking for a meaningful career with a significant impact (Kaspersky, 2018). One way the literature proposes to do so, is through adequate role models. Professional female mentors can help potential students by dispelling myths about the work environment, roles, and responsibilities of a security professional (Pifer, 2017). Pifer mentions that that young women refer to their interest in the areas of security and privacy as stemming from a desire to help people and engage in meaningful work (Pifer, 2017). Therefore, in addition to highlighting benefits, mentors and role models can help guide young professionals and students in determining direction for a future education and career path (Pifer, 2017).

2.5 What are the Effects of Gender Equality?

Women account for half of the global population and, as a result, half of its potential. However, disparity between genders remains an issue today and is impeding societal progress. In order for a change to take place, it is crucial to draw attention to the effects of gender equality and what these can entail for companies and organizations. According to a study conducted by McKinsey & Company, there is a correlation between a company's financial

performance and its level of diversity, which is measured by the number of women and the ethnic and racial variety of its management (Hunt et al., 2015). The study's findings revealed that companies with gender diversity in the top quartile were 15% more likely to achieve financial returns that were higher than the national industry median (Hunt et al., 2015). The correlation showed in Figure 2.6, suggests that companies are more successful when they make a commitment to diverse management (Hunt et al., 2015).

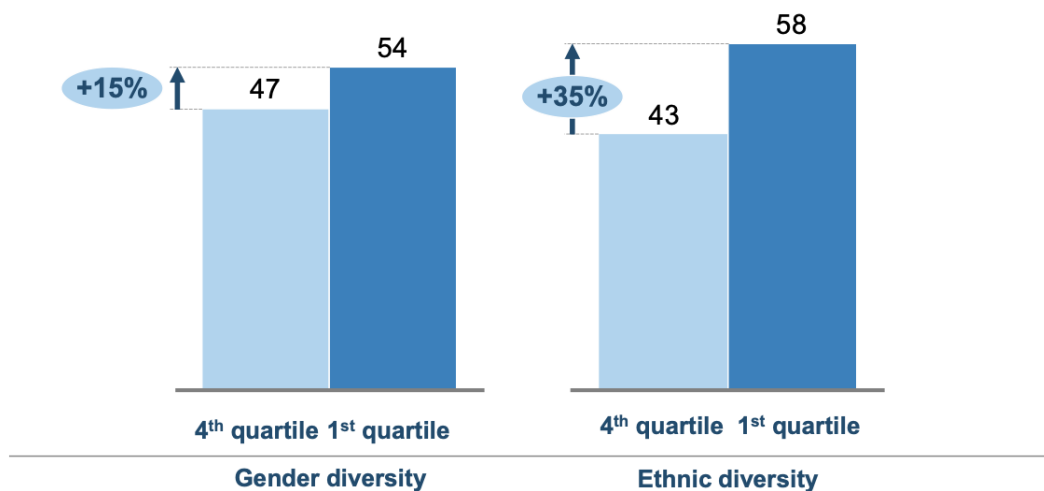


Figure 2.6: The correlation between a company's financial performance and its level of diversity (Hunt et al., 2015)

The context for this discovery was that organizations that embraced diversity outperformed their competitors because it enlarged the talent pool, strengthened customer orientation, boosted satisfaction among employees, improved decision-making, and ultimately improved the company's image (Hunt et al., 2015). Cedric Herring produced a similar finding in his research on the impact of gender diversity and a company's success, discovering effects such as sales revenue, customer count, market share, and profitability relative to competitors (Herring, 2017).

In contrast, Professor Zhang's research on 1,069 top companies in 35 different countries and 24 various industries revealed that gender diversity is only associated with more profitable businesses as assessed by market value and revenue in situations where gender diversity is viewed as "normative" acceptable (Turban et al., 2019). By normative acceptance, we imply a broad societal conviction in the importance of gender diversity (Turban et al., 2019). In other words, gender diversity thoughts produce a self-fulfilling loop. Countries and companies that value gender diversity get the benefits of it (Turban et al., 2019). Zhang and his co-authors believe there are three primary reasons why views about the benefit of diversity contribute so much to the actual value it offers (Turban et al., 2019). These may give lessons for managers who are interested in maximizing the benefits of gender diversity (Turban et al., 2019). The first point to highlight is that a diverse workforce indicates an appealing working environment for talent (Turban et al., 2019).

The second point is that by valuing diversity, you promote the exchange of varied ideas (Turban et al., 2019). Diverse teams are more likely to provide creative ideas. When people from diverse backgrounds collaborate, their distinctive viewpoints frequently foster more innovation, which can result in the production of better products (Turban et al., 2019). Nevertheless, diversity is ineffective without psychological safety (Turban et al., 2019). To get any value out of it, it is crucial to accept that people only offer original ideas to the group when they feel confident enough to speak up and express a competing viewpoint (Turban

et al., 2019). As a result, psychological safety is essential for creative thinking (Turban et al., 2019).

Finally, a varied workforce shows good management to investors (Turban et al., 2019). Gender diversity can also indicate to investors that a company is well-managed (Turban et al., 2019). According to sociological study on market value, investors appreciate when enterprises utilize widely acknowledged "best practices," such as the inclusion of different groups in employment, and they "penalize" those who breach these norms (Turban et al., 2019). In conclusion, it demonstrates that promoting gender diversity as a corporate goal may result in financial rewards and assist a firm in reaching its full potential.

2.6 Summary

As we've seen, the literature identifies a number of possible barriers that prevent women from pursuing careers in cybersecurity. It turns out that in order to increase the number of women in technology careers, it is necessary to nurturing their self-efficacy and interest, remove existing stereotypes, incorrect perceptions and discrimination, demonstrate the various career opportunities, and increase the representation of role models and key influencers. There are currently a lot of intriguing efforts happening to address the underrepresentation of women in the cybersecurity industry. Many of these initiatives center on guiding and connecting girls toward cybersecurity through networking and early exposure to the career path, as well as dispelling myths and increasing the visibility of professional female mentors. Women's entry into a traditionally male-dominated field will increase employment opportunities and help to address labor shortages. Even more crucially, a significant presence of women in the sector indicates a larger chance for growth and innovation, not to mention a more inviting workplace and organizations that put this in focus demonstrate social responsibility.

Chapter 3

Research Approach

The goal of this research is to gain a better understanding of how to address the gender imbalance in the cybersecurity field and the need for new solutions, as well as how to encourage and devise strategies to assist more women in pursuing this career path. The study poses the following research- and sub research question as a solution to that:

- *RQ: "How can the cybersecurity industry entice and retain woman?"*
- *SRQ: "How might the increased representation of female cybersecurity professionals contribute to an organization?"*

When gathering data, both qualitative and quantitative approaches can be used. Using both approaches in a study is sometimes necessary to optimize the investigations and take advantage of the different approaches' strengths. In other cases, using only one of the methods may suffice. Both are legitimate approaches to assess a phenomena in its right context since they both attempt to explain occurrences from many points of view. This chapter argues why the chosen research approach is appropriate for the project and provides justifications for why the alternative research approach is deemed less appropriate.

3.1 Research Design

Research design refers to research plans and procedures that range from broad assumptions to detailed methods of data collection and analysis (Cresswell, 2008). The overall decision involves deciding which design should be used to investigate a topic (Cresswell, 2008). The objective of this case study is to gain a better understanding of the impact of gender equality in the cybersecurity field; to look into what organizations can do to entice and retain women; and to consider how increased representation of female cybersecurity professionals may benefit an organization. As a result, we are focusing on female cybersecurity workers, both managers and other employees, as a target group. Our defined target group is quite narrow due to the underrepresentation of women in cybersecurity, and the use of quantitative methods may have limitations in terms of the sample size of respondents. Furthermore, our goal necessitates more in-depth research that investigates our problem domain with the goal of discovering valuable and possibly novel knowledge, which can be accomplished through qualitative research. This is the basis for deciding to conduct qualitative research through this study, as this approach appears to be best suited for this project.

According to Oates there are three primary case study approaches; exploratory, descriptive, and explanatory (Oates, 2005). When these techniques are used correctly, he claims, they force the researcher to adjust the course of the analysis and the design of the study as needed, ensuring the project's reliability and validity (Oates, 2005). Due to the scarcity of comprehensive studies on gender equality in the cybersecurity field and practical solutions

to this issue, this study is based on a real-life incident. As a result, interviewing personnel from various job positions in the cybersecurity department appeared to be the best way to investigate this issue in organizations. Therefore, an exploratory study would be appropriate for this research project, as Oates defines such a study as being used to define the questions or hypotheses to be used in a subsequent study, as well as to assist a researcher in understanding a research problem (Oates, 2005). It could also be used when there is little information in the literature about a topic, so a real-life instance is investigated to identify the topics to be covered in a subsequent research project (Oates, 2005).

Although according to Oates there are three primary case study approaches, Sarker et al. (2018) presents a map of five prominent qualitative approaches adopted in the IS community, shown in Figure 3.1 (Sarker et al., 2018). As shown in the figure there are many overlaps among the methodologies, and can therefore be hard to understand what genre apply to one's study (Sarker et al., 2018). As the figure shows, an exploratory case study tends to involve inductive reasoning (Sarker et al., 2018). As a result, the goal of using the inductive approach is to allow research findings to emerge from frequent and dominant themes inherent in transcription while avoiding the constraints imposed by more structured methodologies.

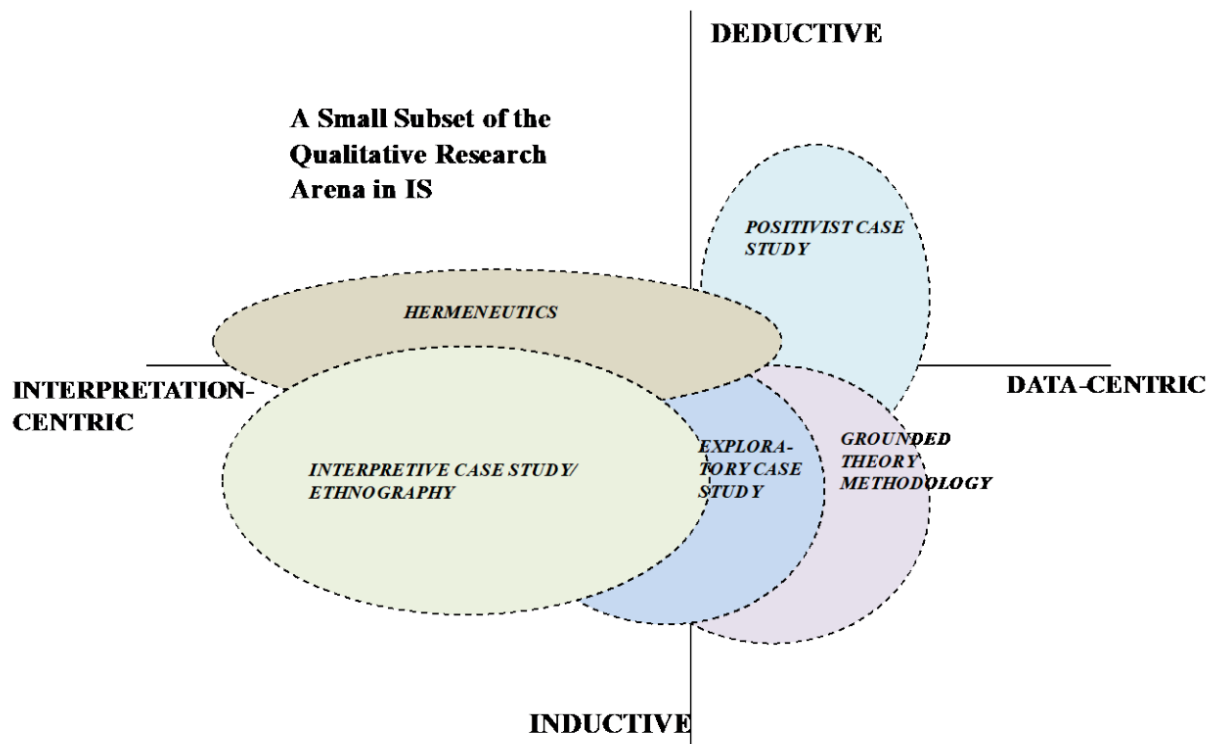


Figure 3.1: A map of genres in qualitative research (Sarker et al., 2018)

3.2 Qualitative Approach

Qualitative research in the field of information systems is a large umbrella terminology that encompasses many techniques and philosophies, making it difficult to define (Hennink et al., 2020). In general, qualitative research is a approach that allows for in-depth investigation of people's experiences through the use of numerous research techniques ranging from interviews and observations to archival research (Hennink et al., 2020). One of the most distinguishing characteristics of qualitative research is that it helps you to identify issues from the perspective of your study participants and comprehend the meanings and interpretations that they assign to behavior, events, or objects (Hennink et al., 2020). Qualitative researchers investigate people in their natural settings to establish how the context of their life, such as the social, economic, cultural, or physical context in which they live, affects their behaviors and experiences (Hennink et al., 2020). As a result, qualitative research seeks to embrace and comprehend contextual impacts on research issues (Hennink et al., 2020), and, as Denzin and Lincoln stated, qualitative research entails an interpretative and naturalistic approach to the world (Denzin and Lincoln, 2008) .

Gender equality in cybersecurity is a challenging topic to hypothesize, as proven by the research, because it includes investigating the subjective enterprise and social context. One may argue that merely reviewing the literature would suffice to establish a theory concerning the phenomena. Nonetheless, we believe that there is a gap in the research in this field that has to be filled. Qualitative research provides various advantages, including more design flexibility, the capacity to avoid depending on the researcher's preset assumptions, the ability to present findings in greater depth and complexity, and the opportunity to imitate participants' unique personal experiences (Griffin, 2004). As a result, we determined that a qualitative approach would be appropriate.

Interviews were the method of choice because they allow participants to elaborate in ways that are not feasible with other approaches, such as survey research. We have greater freedom when using the qualitative interview approach (Jacobsen, 2015). This means that we may uncover unexpected new events throughout the interview (Jacobsen, 2015). Based on these occurrences, we may opt to change the investigation's problem, data gathering method, and analysis (Jacobsen, 2015). We have less leeway when conducting a quantitative research approach since we must follow certain stages and procedures (Jacobsen, 2015). This sort of research is more strict and will offer less chance for alterations along the way (Jacobsen, 2015). In light of their transparency, we can thus claim that using qualitative interviews is a great choice for our research. Considering our lack of expertise with the topic, such an approach is a suitable place to start since it allows for the development of new theories and ideas.

To validate our methodological approach, we incorporated a comparison of qualitative and quantitative research methods from the book "Qualitative Research Methods," as shown in Figure 3.2, in which Hennink and his co-authors highlight the key distinctions (Hennink et al., 2020).

| | Qualitative research | Quantitative research |
|-------------------------|--|--|
| Objective | To gain a contextualized understanding of behaviours, beliefs, motivation. | To quantify data and extrapolate results to a broader population |
| Purpose | To understand why? How? What is the process? What are the influences or context? | To measure, count, or quantify a problem. To answer: How much? How often? What proportion? Which variables are correlated? |
| Data | Data are words (called textual data) | Data are numbers (called statistical data) |
| Study population | Small number of participants; selected purposively (non-probability sampling) | Large sample size of representative cases |
| | Referred to as participants or interviewees | Referred to as respondents or subjects |
| Data collection methods | In-depth interviews, observation, group discussions | Population surveys, opinion polls, exit interviews |
| Analysis | Analysis is interpretive | Analysis is statistical |
| Outcome | To develop an initial understanding, to identify and explain behaviour, beliefs or actions | To identify prevalence, averages and patterns in data. To generalize to a broader population |

Figure 3.2: Differences between quantitative and qualitative research methodologies (Hennink et al., 2020)

3.3 The Unit of Analysis and Subject Selection

This exploratory study seeks to investigate how gender equality affects the cybersecurity sector, as well as various strategies for attracting and retaining women in the field, and how an increased representation of female cybersecurity professionals can benefit an organization. To get the best answers and investigate different measures, we needed to understand the various experiences that women in the field have had and are experiencing. As a result, we decided to examine the research questions from a female perspective. We reached out to female cybersecurity professionals in various organizations for collaborations and interviews. The strategy was to interview female cybersecurity candidates from various backgrounds and titles, and we wanted candidates from multiple organizations to avoid bias. As a result, different roles of relevance within the organizations were interviewed in order to provide a rich and broad picture of the phenomenon in the chapter of empirical findings.

We reached out to our contacts in various cybersecurity organizations and expressed our interest in interviewing women in this field. We wanted to interview regardless of role because there are so few women, even though a mix of managers and employees would be ideal. This resulted in a total of 14 interviews, all of which contributed significantly to our research. We wanted to protect the respondents' and their employers' anonymity so they could answer honestly without fear of repercussions. As a result, Table 3.1 depicts our respondents' roles and years of employment, using pseudonyms to maintain anonymity. The results revealed a wide range of experience and areas of responsibility among them, providing different perspectives on the answers from the interviews.

| Respondent | Pseudonym | Role | Years in role |
|---------------|--------------------------|--|---------------|
| Respondent 1 | CISO | Chief Information Security Office | 1 year |
| Respondent 2 | PHD_Student & Consultant | PHD student in how one can handle and understand cybersecurity, and consultant | 7 years |
| Respondent 3 | Manager_CEO | (CEO) Manager | 14 years |
| Respondent 4 | PHD_Student | PHD student in cybersecurity with focus on digital supply chains | 2 years |
| Respondent 5 | Consultant | Consultant in cybersecurity | 3 years |
| Respondent 6 | TeamLead_NOC | Part of a management team at operation center | 2 years |
| Respondent 7 | Senior_Manager | Senior IT transformation manager | 2 years |
| Respondent 8 | Advisor | Risk and audit advisor | 3 years |
| Respondent 9 | Manager_Consultant | Consultant manager | 2 years |
| Respondent 10 | Senior_Advisor | Senior advisor | 4 years |
| Respondent 11 | Manager_Cosultant | Head of consulting | 2 years |
| Respondent 12 | Advisor | Cybersecurity advisor | 1 year |
| Respondent 13 | Advisor | Security advisor | 2 years |
| Respondent 14 | Manager_Consulting | Cybersecurity consulting manager | 4 years |

Table 3.1: Subject selection

3.4 Data Collection

The important issue in conducting qualitative research is the quality of data obtained, which is based on the technique of data collecting employed. Interviews, unlike other methodologies, have distinguishing features which make them superior. As said by Berg, "*the value of interviewing is not only because it creates a holistic image, analyzes words, and gives specific opinions of informants; but also because it allows interviewers to speak in their own voice and convey their own thoughts and feelings*" (Alshenqeeti, 2014). Interview styles vary greatly, but they all have one thing in common: they use questions to learn about people's ideas, feelings, beliefs, and behaviors (Stuckey, 2013). By using interviews in our research, we may gain a deeper understanding of why participants feel the way they do regarding gender equality in the cybersecurity industry. Knowing the "why" can help us to delve further into the motivations that push both men and women into this industry. The process of determining how to format our interviews began with a study of current research, as outlined in the preceding chapter. The literature study was required to assure the higher reliability and accuracy of the questions to be asked. Understanding past study findings helped to modify the questions in a way that added value to the research.

Generally, it is common to distinguish between three types of interviews: unstructured, semi-structured and structured interviews (Lune and Berg, 2017). Their main distinction is how much influence the interviewer has over the conversation and the interview's aim (Lune and Berg, 2017). Berg and Lune presented the various interview variants in their book "Qualitative Research Methods for the Social Sciences" and can be seen in the Table 3.2 (Lune and Berg, 2017). Because of two key considerations, we chose semi-structured interview as our technique of choice. The first point is that this technique of data collecting is best suited for studying interviewees' opinions and thoughts about our issue through two-way dialogue.

Performing SSIs allows us, as interviewers, to follow-up with additional questions to clarify the answers. The second point to consider is that this technique is suitable for delving deeply into our topic and properly comprehending the answers that are given (Harrell and Bradley, 2009).

| Standardized Interviews | Semi-standardized Interviews | Unstandardized Interviews |
|---|---|--|
| Most formally Structured | More or less structured | Completely unstructured |
| No deviations from question order | Questions may be reordered during the interview | No set order to any questions |
| Wording of each question asked exactly as written | Wording of questions flexible | No set wording to any questions |
| No adjusting of level of language | Level of language may be adjusted | Level of language may be adjusted |
| No clarifications or answering of questions about the interview | Interviewer may answer questions and make clarifications | Interviewer may answer questions and make clarifications |
| No additional questions may be added | | |
| Similar in format to a pencil-and-paper survey | Interviewer may add or delete probes to interview between subsequent subjects | Interviewer may add or delete questions between interviews |

Table 3.2: The various interview structures (Lune and Berg, 2017)

3.4.1 Interview Methodology

To ensure that the interview guide was constructed in the best possible way, we decided to adhere to Kallio’s framework for developing a semi-structured interview guide, depicted in Figure 3.3 (Kallio et al., 2016).

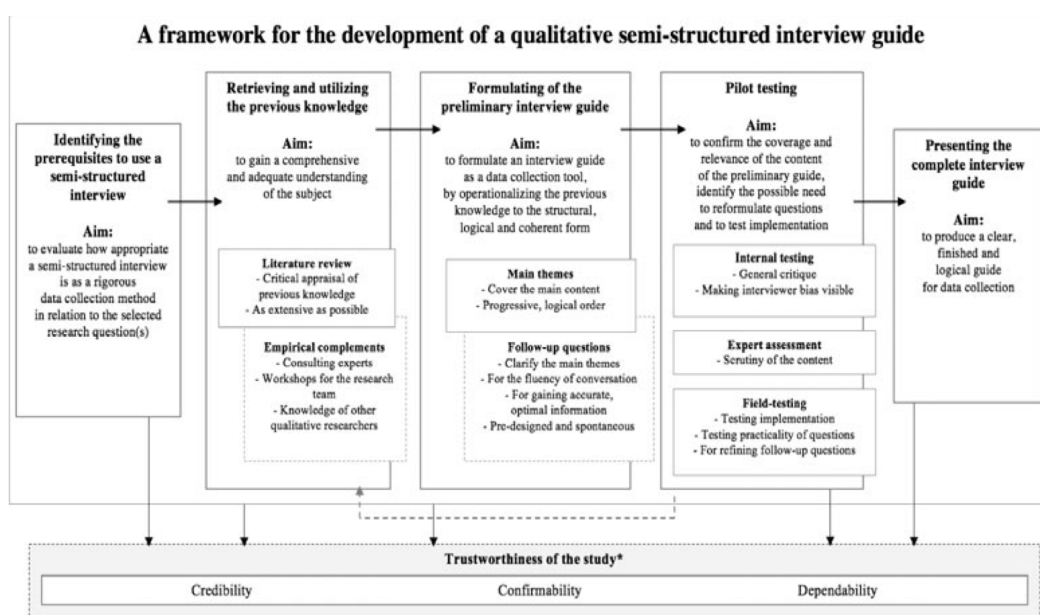


Figure 3.3: The stages of semi-structured interview guide (Kallio et al., 2016)

The framework is divided into five stages, the first of which involves identifying the prerequisites for using semi-structured interviews (Kallio et al., 2016). As previously discussed, semi-structured interviews suited our selected research questions very well and the benefits and drawbacks of utilizing this method were carefully considered throughout the process. The framework's next stage involves retrieving and using previous knowledge (Kallio et al., 2016). A systematic literature review was carried out in order to gain a comprehensive understanding of the selected topic, which assisted in the construction of the preliminary interview guide, the framework's third phase. As stated by Kallio and his co-authors, it is important that we understand the research's substance (Kallio et al., 2016). Furthermore, to determine whether the questions were pertinent or whether they needed to be rewritten, a pilot test was conducted after the first draft was finished. The preliminary interview guide received feedback from experts in the field, which was essential for comparing the interview guide's material to the goal and the topics to be covered. The intention of this step was to validate the coverage and relevancy of the preliminary guide's content (Kallio et al., 2016). Following the completion of the fourth stage, it was possible to make informed changes and adjustments to the interview questions, resulting in the final edition of the interview guide A and the completion of the framework's fifth and last stage.

3.5 Limitations of Interviews

A semi-structured interview has many advantages and possibilities, but it can also have some drawbacks. Table 3.3 outlines the limitations and solutions with the qualitative methodology based on a list from Myers and Newman (2007) of the most common concerns about doing qualitative interviews:

Table 3.3: Limitations and potential solutions with semi-structured interviews

| Limitations | Solutions |
|---|--|
| <p>Artificiality of the interview: The qualitative interview entails questioning a complete stranger; it entails asking subjects to give or create opinions under time constraints.</p> | <p>Explain the process in detail to interviewees who may be nervous about being interviewed. Share interview questions with participants ahead of time so that they can prepare.</p> |
| <p>Lack of trust: Because the interviewer is a complete stranger, the interviewee is likely to be concerned about how much the interviewer can be trusted. This means that the interviewee may choose not to reveal "sensitive" information. If this is potentially useful information for the research, the data collection is still incomplete.</p> | <p>Explain in advance how information will be handled, stored, and deleted. Make sure you have an accepted NSD application and a consent form for the interviewee to sign.</p> |
| <p>Lack of time: Due to a lack of time for the interview, data collection may be incomplete. However, it can also lead to the opposite issue of subjects forming opinions under time constraints (when these opinions were never really held strongly to start with). More data are gathered in this case, but the data gathered is not entirely reliable.</p> | <p>Create well-defined questions that can be effectively answered and understood by the interviewee.</p> |

Continued on next page

Table 3.3: Limitations and potential solutions with semi-structured interviews (Continued)

| | |
|---|---|
| <p>Elite bias: A researcher may only interview a few high-ranking people (key informants), missing out on gaining a comprehensive understanding of the situation. In other words, interviewing a company's "stars" may introduce bias into qualitative research. Data from articulate, well-informed, typically high-status informants is overrepresented, while data from less articulate, lower-status informants is underrepresented.</p> | <p>Interview people in various roles and positions from multiple organizations to get various perspectives and to avoid bias.</p> |
| <p>Constructing knowledge: Interviewers may believe they are simply absorbing data or information, unaware that they are actively producing knowledge. This can happen when an interviewee reflects on a question they've never thought about before, and the interviewer takes that contemplation and turns it into something logical and consistent, but not what the interviewee reflected on.</p> | <p>Thank the interviewee for their time, and let them know they contributed something to your project.</p> |
| <p>Ambiguity of language: Words can be ambiguous, and what the interviewer asks may differ from what the interviewee hears, resulting in miscommunication between the interviewer and the interviewee.</p> | <p>Make certain that the questions are well-formulated and understandable for the interviewees.</p> |
| <p>Interviews can go wrong: Fears, problems, and pitfalls abound in interviews. It is possible for an interviewer to offend or inadvertently insult an interviewee, in which case the interview may be terminated.</p> | <p>Send the interview guide to the interviewee ahead of time so they know what to expect.</p> |

All of the challenges described in Table 3.3 are well-known difficulties that can arise when conducting qualitative research. According to Myers and Newman (2007), researchers should be more aware of the potential problems and downfalls associated with the use of qualitative interviews (Myers and Newman, 2007). The qualitative interview is a highly effective data collection tool, but those who use it should be aware of its advantages and disadvantages. Before beginning the interviewing process, the limitations listed above were examined and taken into account. An interview guide and consent form were also created and distributed to each subject to aid in the development of trust between interviewers and interviewees. The purpose of the guide and consent form was to inform the interview objects about how the data they provided would be handled, stored, and erased.

3.6 Data Analysis

Following the completion of 14 interviews with representatives from multiple companies involved in cybersecurity in Norway, the process of analyzing the collected data began. We were satisfied with the amount of interview responses at this point when respondents began to repeat themselves and it did not result in any new themes, indicating that we had reached data saturation. We decided to use Teams' built-in transcribing feature in addition to recording the interviews rather than taking notes so we could focus entirely on them while also saving time. This performed fairly well, however we had to make a few adjustments because the program's built-in transcribing didn't pick up all the words that were stated.

The reviewed transcribed documents were then evaluated and coded in NVivo, a software program for qualitative research. Our need to analyze unstructured data from our semi-structured interviews made it suitable to use NVivo since it offers ways to gain a general sense of what themes exist in the data and also enables you dig into the information for more in-depth analysis.

As one of the characteristics of qualitative analysis is its high complexity, we decided to employ the same framework as the "National Science Foundation" used because they were successful in identifying some significant shared elements for qualitative analysis (National Science Foundation (NSF), 1997). The aim of our data analysis was to identify and comprehend key patterns that would assist us in answering our research questions. We were able to effectively complete our data analysis and uncover and comprehend crucial patterns that would aid in answering our research questions by adhering to the steps of the aforementioned framework, namely data reduction, data display, and conclusion drawing and verification (National Science Foundation (NSF), 1997). Data reduction, according to the NSF, is the process of "selecting, focusing, simplifying, abstracting and transforming the data that appear in transcriptions" in order to make the data more manageable and intelligible in light of the issues being addressed (National Science Foundation (NSF), 1997). The data obtained from the semi-structured interviews needed to be rationally reconfigured and organized. Because of this, NVivo was utilized to code the raw data obtained from the semi-structured interviews, making it easier for us to leave out information that was irrelevant. Our research questions were utilized to filter out extraneous information, resulting in the exclusion of useless data.

NSF describes data display as the framework's second element, which is centered on providing "an organized, compressed collection of information that enables conclusions to be made" (National Science Foundation (NSF), 1997). Using NVivo, higher level categories and themes that were identified from the obtained data were displayed as nodes, highlighting systematic patterns and relationships in the data. The procedure of showing data has enhanced our research, by enabling us to meticulously visualize the data we have gathered in order to make valid conclusions. Using our main research question, "how can the cybersecurity entice and retain woman?" as our starting point, the example below shows how we handled this. The nodes represent themes and categories from the data collected. As seen in Figure 3.4, nodes are listed in NVivo as "name".

| Name | ^ | Files | References |
|------------------------------|---|-------|------------|
| ▼ ○ Proposed measures | | 0 | 0 |
| ○ Flexibility | | 2 | 2 |
| ○ Overcoming stereotyp... | | 7 | 9 |
| ○ Role models | | 3 | 5 |
| ○ Showing possibilities a... | | 13 | 19 |
| ○ Taking inspirations fro... | | 1 | 1 |

Figure 3.4: NVivo data analysis

Conclusion drawing and verifying is the framework's third and final element, and it entails delving deeper into the significance of each piece of information and the potential implications for the chosen questions (National Science Foundation (NSF), 1997). We aim to ensure that the data and conclusions may be established reasonably. The validity in this case is justified by credibility, defensibility, warrantedness, and how well equipped the conclusion is to withstand alternative explanations (National Science Foundation (NSF), 1997). This

was accomplished by verifying the data and cross-checking it with the conclusions that were formed. To help strengthen the integrity of our conclusion from the qualitative study analysis, we asked stakeholders in the cybersecurity industry to contribute their perspectives, experiences, and knowledge on the selected topic. Integrating supervisors into the validation process has been crucial to ensuring increased quality in the work with the conclusions and the robustness of our findings against alternative interpretations.

3.7 Ethical Considerations

When conducting interviews with cybersecurity professionals, confidentiality must be taken into account. Although the interviews do not collect much sensitive information, there are some that must be protected, such as names, organizational roles, responsibilities, and contact information. In order to protect this information, the interview recordings are stored on secure cloud storage provided by the University of Agder. The interviewees have the right to see and revoke their permission to see the data stored about them at any time. During each interview, we were clear about what would be recorded, where it would be stored, and when it would be erased.

In order to collect and store information from the interviews, it was necessary to submit an NSD application prior to conducting the interviews. The Norwegian Center for Research Data (NSD) is in charge of managing all research projects and maintaining a research data archive (Sikt, 2023). Once the NSD has approved their application, researchers are legally permitted to preserve and document their data (Sikt, 2023). As a result, we were cautious to obtain NSD's permission before storing or documenting any data in this study. All interviewees were aware that our NSD application had been accepted, and they all willingly signed an agreement with the provided information. Prior to the interview and recording, all parties were aware of each other's requirements and consent.

Chapter 4

Empirical Findings

The findings drawn from the data analysis of the semi-structured interviews are presented in the following section. The aim of the empirical findings is to respond to our RQs by illustrating the results and providing quotes from our fourteen informants that demonstrate our findings.

Table 4.1 displays the total number of participants interviewed, their roles, and the percentage of female cybersecurity professionals in their organizations. As the table illustrates, there is still work to be done to enhance gender diversity in the cybersecurity industry, with organization four having the largest percentage of women at 40%, and organization three having the lowest ratio of females at only 10%. This highlights the importance of developing new strategies to attract and retain women in the profession. In this chapter, we will look at the findings of the interviews, such as the reasons why women are underrepresented in cybersecurity, proposed measures from the interviewees and their thoughts on the effects of gender equality.

| | |
|--|--------|
| Total participants | 14 |
| <i>Roles:</i> | |
| Chief Information Security Officer (CISO) | 2 |
| Manager | 5 |
| Consultant | 2 |
| PHD Student | 1 |
| Advisor | 4 |
| <i>Total percentage of female cybersecurity professionals in the various organizations:</i> | |
| Organization 1 | 15-20% |
| Organization 2 | 23% |
| Organization 3 | 10% |
| Organization 4 | 40% |
| Organization 5 | 29% |
| Organization 6 | 20% |
| Organization 7 | 20% |

Table 4.1: Summary table of the interviewees

4.1 Why Women are not in Cybersecurity

The findings of our qualitative approach identified various reasons why women are under-represented in cybersecurity. One of the questions posed to the respondents was, "What do you see as the most significant barrier to overcome for more women to pursue a career in cybersecurity?". According to the responses of our respondents, several of the challenges are related to the barriers identified in the literature, demonstrating the legitimacy of the barriers.

4.1.1 Self-efficacy, Interest and Characteristics

In addition to the fact that several of the respondents have personally experienced this, some of the respondents indicate the fear of not being competent enough or not knowing enough about technology might be a barrier for girls considering this career path. In reply to the question, "*Was there something that almost made you change your mind about the cybersecurity sector?*" respondent one stated:

"Fear of not understanding technology well enough, something I can still identify with, especially when the sector sends messages about patching and similar topics. My IRT team will be able to grasp this, but asking what that means, why there is an issue, what is this, or can you explain this more simply seems a little out of place. That I lack a comprehensive knowledge of technology."

When asked, "*What would be your most crucial piece of advice to women contemplating a career in cybersecurity?*" she continues:

"Actually, it's having confidence in your abilities. I believe it will be a while before we girls step up and declare, "I can do this," and that we truly must dare to say, "Now that I have an education, I know about this or that, and I wrote a paper about such and such. As for me, I am not very good at technology, but I am very good at applying technology and know a lot about insight work and intriguing impact and change management, as well as conveying risk knowledge and explaining procedures. In a sense, develop self-assurance or discover your strengths and concentrate on them rather than putting your energies on your weaknesses"

In other words, if one recognizes and concentrates on their strengths, one will considerably improve their chances of success and develop more self-confidence. Additionally, throughout the first year of her bachelor's degree, respondent three shared her feelings of not being competent enough and expressed skepticism about her ability to work in cybersecurity. She expressed the following:

"I just want to say that during the first six months of my bachelor's degree in computer programming, when you hadn't touched a PC and where there are about five girls and 110 boys, and all the boys had played computer games for many years, I was absolutely certain that I would get to fail in all subjects compared to the other students in the class. Just a few of us were female. But while I was studying, the boys were playing games, and when it came time for the first exam, I performed well, possibly better than many other students who hadn't been paying attention. However, in the first half, I was probably on the verge of quitting."

This shows that having no prior experience in the security field is not a requirement for achievement in this industry and refutes the notion that cybersecurity is only for men. However, more importantly, it shows that even a feeling of mastery may spark an interest, which, for this respondent, was vital in her decision to continue with her bachelor's degree. Low self-efficacy might thus operate as a barrier for girls, as respondent 3 explained:

"Many people require encouragement that they are capable of accomplishing things. Girls might need a bit more encouragement to believe in their own abilities, whereas boys are more likely to say, "Yes, we can try that or let's see". Because of their slightly distinct characteristics, it is crucial that you actually treat them a little differently. Girls frequently need to make sure that the employer will not be disappointed. Despite the fact that they may be extremely talented and intelligent compared to many others, they don't sell themselves because they are upfront about their limitations and go a little too far in asserting that they can't. As a result, if you manage to bring in two boys and two girls for an interview, you should be aware that the girls usually spill everything, while the boys talk about everything they can. Then this will seem very different if you take notes. That's where I wish girls were better, if just to be neutral and not tell everything they can't. I saw girls read this list as if it were a point rather than a list of prerequisites in a job advertisement. Then there comes a point where they can't, they don't apply."

Men and women must therefore be addressed differently because they each have distinctive characteristics. While men have strong self-efficacy and believe they can achieve anything, which increases their interest in cybersecurity, women are more faster to doubt their abilities, resulting in low self-efficacy and reduced interest in the subject.

4.1.2 Stereotypes, Perceptions and Discrimination

Many of the respondents agree that gender stereotypes, perceptions, and discrimination exist in the cybersecurity industry and that this discourages women from entering the field. Due to the stereotype that cybersecurity is largely a male job, many women don't think of it as a career option. According to respondent five, we have to *"eliminate the idea that IT is primarily a boy's subject to improve the proportion of women working in the cybersecurity sector"*. Respondent five adds that the media frequently reinforces this stereotype in her response to the question, *"how to encourage more women to pursue careers in cybersecurity"* and said the following:

"Many people who hear IT envision men sitting in hoodies typing green code on a screen. In other words, you don't think of it as being like a typical consultant who wanders around, gives a presentation here, and then performs these kinds of things. It's about demystifying the IT sector just a bit because, in my opinion, we have a peculiar relationship with what IT is. Since there aren't as many of those kind of people as I had imagined—people who hang out in black hoodies and doing programming."

That's not exactly the picture that would entice a more diversified pipeline and it simply signals that an alteration in how cybersecurity is presented is required. In support of the need for a shift in how cybersecurity is viewed, respondent twelve expressed the following:

"This is not going to be a desirable job choice as long as women think of this industry as being full of sweaty "gamers" or nerdy IT professionals who may not know how to relate to women or maybe look down on women."

Women are less likely to pursue cybersecurity professions because they do not identify with these stereotypes, which is absurd given that cybersecurity offers many fulfilling career choices and possibilities for women. We can contribute to dispelling these stereotypes and eliminating the so-called *"boys club"* that respondent one still finds in certain areas, as well as the linguistic stereotype that respondent two has heard *"the guys at the operations center"* by raising awareness of the many talents and backgrounds required for cybersecurity.

The respondents all concur that there is a clear perception of poor female presence in the cybersecurity industry, and many of them believe this is due to conventional gender roles shaped by the general public. As respondent two notes, *"There is really no specific reason why it is a profession that causes an overrepresented in either direction. It's not that men and women have particularly distinct prerequisites, but perhaps that still exists to some extent in society"*. Respondent three describes the occupations that women most frequently apply for and the reasons behind this:

I think girls have a stronger propensity to gravitate toward caring professions, social occupations with a higher percentage of people, because they desire human integration, which perhaps cybersecurity does not. It can come off as a bit more lonesome. It may appear uninteresting. Instead, we must demonstrate that a significant portion of cybersecurity has to do with personnel routines and behavior, training for the human element as opposed to the requirement that you be an expert with a technical tool.

Due to the above, women are more likely to choose social work or related fields than traditionally masculine careers. Although cybersecurity contains these elements that women prefer, this is not clearly demonstrated as the respondent three claims. Additionally, many women decide against pursuing a career in cybersecurity because of discrimination in the field. A few of the respondents had heard about instances of discrimination in the sector, and some had even encountered situations in which they had been victim of it. Regarding having experienced discrimination, interview respondent one added the following :

This happened to me once at a conference with security managers from large regional and national companies. Nobody was interested in who I was. It took me some time to introduce myself, and when I did, they were shocked to discover that I was one of them. That bothered me, especially because it was our first meeting with the network outside of the office. It was interesting, but also a bit perplexing because it wasn't how it should have been.

4.1.3 Career Opportunities

Even though cybersecurity is one of the fastest growing professions, women continue to be underrepresented in the industry. During the conducted interviews it emerged that the respondents had differing perspectives on the barriers to women's career opportunities in cybersecurity. One of the potential impediments is being exposed to cybersecurity and its job opportunities too late in life. Respondent two agrees with this, saying, *"I didn't consider it realistic until I arrived here and was exposed to it throughout my working life. It wasn't until then that I realized this was a possible possibility for me"*. Respondent five concurs with this and adds, *"The challenge, I believe, is that you must discuss IT and online security earlier. Of course, you can't go up to a six-year-old and start talking about encryption. So you have to figure out a way to communicate about it that works"*. She then continues, *"Perhaps enter secondary school, and talk about exciting options and occupations in cybersecurity, even if they are probably not at the level where they have thought that far yet"*.

Another major theme that emerged from the responses was the need for more than just technical qualifications in cybersecurity. There is a widespread misperception that cybersecurity entails solely highly technical characteristics, as well as misconceptions that one must be a programmer or a hacker to work in this profession. Respondent seven supports this observation by giving this statement:

"Returning to what we were discussing, you can work in cybersecurity even if you don't have a technical education or are a developer. Although we need a lot of

them, there are other things you can execute that don't require a technical expertise. That, I believe, will be an important first step toward recruiting more women".

Respondent eight agrees with the preceding quote. She is also passionate about bringing more women into the industry, and she has her own ideas about which areas of cybersecurity might be more appealing to women. She expands on the previous quote by mentioning additional aspects of cybersecurity that she believes are essential in the field:

"The nice thing about cybersecurity is that there is such a broad range that you need everyone from those who are highly skilled at deep technical to those who are good at having solid structure and reach towards project or management, security management, and administrative. Women are frequently better at structure and organization than males, so having both skill sets is essential".

Finally, the majority of respondents agree and conclude that women have excellent opportunities in cybersecurity if they are willing to pursue it. Some claim that regardless of gender, the opportunities are equal. Others believe that women are in a unique situation in which they can take advantage of the fact that they are a minority in this industry, as interviewee twelve believes:

"Women, in my opinion, have excellent potential in cybersecurity today. Right now, I believe we are in a unique position in that organizations in cybersecurity are increasingly focusing on recruiting more women, yet very few women are studying this profession. I believe this signifies that those of us who have chosen this career option have and will continue to have a lot of options in this profession".

4.1.4 The Impact of Role Models and Key Influencers

During the interviews, some of the respondents shared their experiences of familiar encouragement. They emphasized the role of key influencers, which includes family members, in sparking an interest in cybersecurity. *"I grew up in a family that was quite interested in the subject. I have a father and sister in the IT field, so it's definitely a combination of heritage and environment"* interviewee one explains. Respondent five was raised in a similar manner, however her family always encouraged her to pursue her own interests:

"Yes, my father is a civil engineer, a mechanical engineer, therefore he most likely had a significant influence on my decision to pursue a career in engineering. But I've always been encouraged to pursue my own interests, and I've been pretty clear about what direction I wanted to go. So I've received a lot of support for what I've chosen, and dad has helped me when I've been stuck with mathematics. I've got their support for the decisions I've taken, and no one has been surprised that I went into IT, because I think it was relatively natural".

Several other respondents emphasize the absence of role models in the industry and the importance of this in attracting more females to the profession. Respondent three also comments on the importance for every woman in the profession to promote cybersecurity, *"As ambassadors, we also have to go out and educate about this"*. Respondent eleven however, discusses the importance for girls to build each other up and to stand together. In a male dominated industry women need to encourage each other and not tear each other down.

"I believe we girls need to help one another even more. Unfortunately, I have been in situations where the girls do not support one another. I've been very keen on doing the opposite, that is, cheering people on, using LinkedIn to pay tribute to one another, and hosting events like Security Divas, because I believe it's important that we demonstrate that there are more people in the industry, and that it's okay to be different, even as a girl. It's difficult to be the first. Or being one of the few, which I believe is what many find difficult".

4.2 How can the Cybersecurity Entice and Retain Woman?

The findings of our qualitative research provided important insight into the challenges that the cybersecurity sector faces in attracting and retaining female professionals. One of the semi-structured interview questions was, "What do you think it will take for more women to choose to study and work in cybersecurity?". The majority of the respondents proposed one or more measures for increasing the number of women in the profession. According to the data, the top five measures offered by respondents were:

1. Showing possibilities and raising awareness
2. Overcoming stereotypes and misconceptions
3. Role models
4. Flexibility
5. Taking inspiration from other male dominated professions

The sunburst chart in Figure 4.1 depicts the measures offered by the respondents. Because each respondent could provide one or more measures, the chart shows which measures received the highest ratio of answers. As a result, the chart is not based on percentages. And as seen in the blue section, most respondents advocated and agreed on showing possibilities and raising awareness. This measure aims to promote cybersecurity early in life, so that it affects women at a younger age. It is also about highlighting and informing what cybersecurity is and entails. Respondent five mentions that: "More individuals need to study cybersecurity, and the profession has to be promoted earlier", which several of the other respondents agrees with. She then continues: "We can promote cybersecurity as much as we want at universities, but an imbalanced distribution has already occurred there, right? So I believe we ought to start earlier". Although many respondents agree, the most frequently repeated response is to educate on what cybersecurity entails and the various skills and perspectives required in this profession, as respondent four expresses: "It needs to be more actualized for women so that it isn't just the technical standpoint that is highlighted. But also demonstrate that there is a human perspective here".

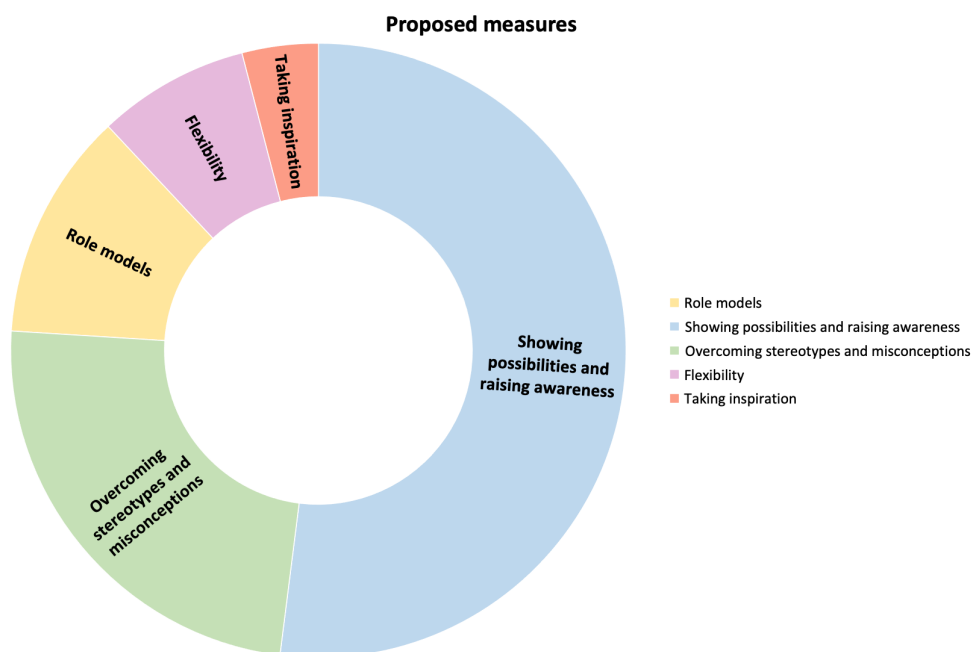


Figure 4.1: Proposed measures to entice and retain women in cybersecurity

Overcoming stereotypes and misconceptions is the measure with the second highest ratio of responses. This entails that there are many misconceptions and prejudices concerning the profession and its practitioners. Interviewee five adds to this with her take on the stereotypes: *"I think a lot of people who hear IT imagine those people in movies sitting in a hoodie in the basement typing green code on a screen"*. Several respondents also stated that it is widely believed that people working in cybersecurity must be programmers or ethical hackers. The stereotypes and misconceptions of IT and cybersecurity contribute to less understanding of what it actually entails. Respondent five continues, *"I think we need to demystify the IT industry"*.

Even though they have a lower response rate, the next three measures are as important in the pursuit of attracting and retaining more female cybersecurity professionals. Role models and key influencers, flexibility in terms of working hours and location, and taking inspiration from other male dominated professions, are all critical measures to implement to increase gender equality in the profession.

4.3 The Value of Female Participants in Organizations

In order to address our sub-research question, *"How might the increased representation of female cybersecurity professionals contribute to an organization?"* we decided to ask our interviewees, *"Do you think gender equality will have an impact in the workplace?"*. The answers to this question are illustrated in the treemap diagram in Figure 4.2, which shows the beneficial outcomes that gender equality will have, according to the respondents. This diagram, like the one in the previous section, is based on the fact that interviewees are given the option to offer one or more answers to the same question, and in this context express one or more effects that gender equality would have. As a result, the figure illustrates effects depending on the number of times they have been suggested rather than as percentage. As seen in the diagram, our fourteen interviewees expressed four effects, which are as follows:

1. Better working environment
2. Multiple perspectives and viewpoints
3. Wider talent pool
4. Improved collaboration

The two most noticeable effects were "better working environment" and "multiple perspectives and viewpoints," with the former mentioned by 9 out of 14 respondents. This effect assumes that an gender equal working environment creates a more favorable workplace with increased job satisfaction. Several respondents state that a gender-equal workplace benefits everyone because it provides a different dynamic and keeps the so-called "boy atmosphere" at bay. As respondent twelve said, *"First of all, I think it becomes a more attractive workplace for other women when you have gender equality because you avoid the so-called "boy atmosphere" where you can unfortunately experience inappropriate jokes or topics of conversation"*. Respondent one adds, *"gender equality can have something to say for the working environment because many lunch conversations are about open AI, and there aren't that many who talk about topics that are interesting to a girl"*. This implies that the majority of respondents see the value of an gender equal workplace, and the conclusion of interviewee two's response, *"If we had zero girls, it would have been a worse environment,"* aligns well with this.

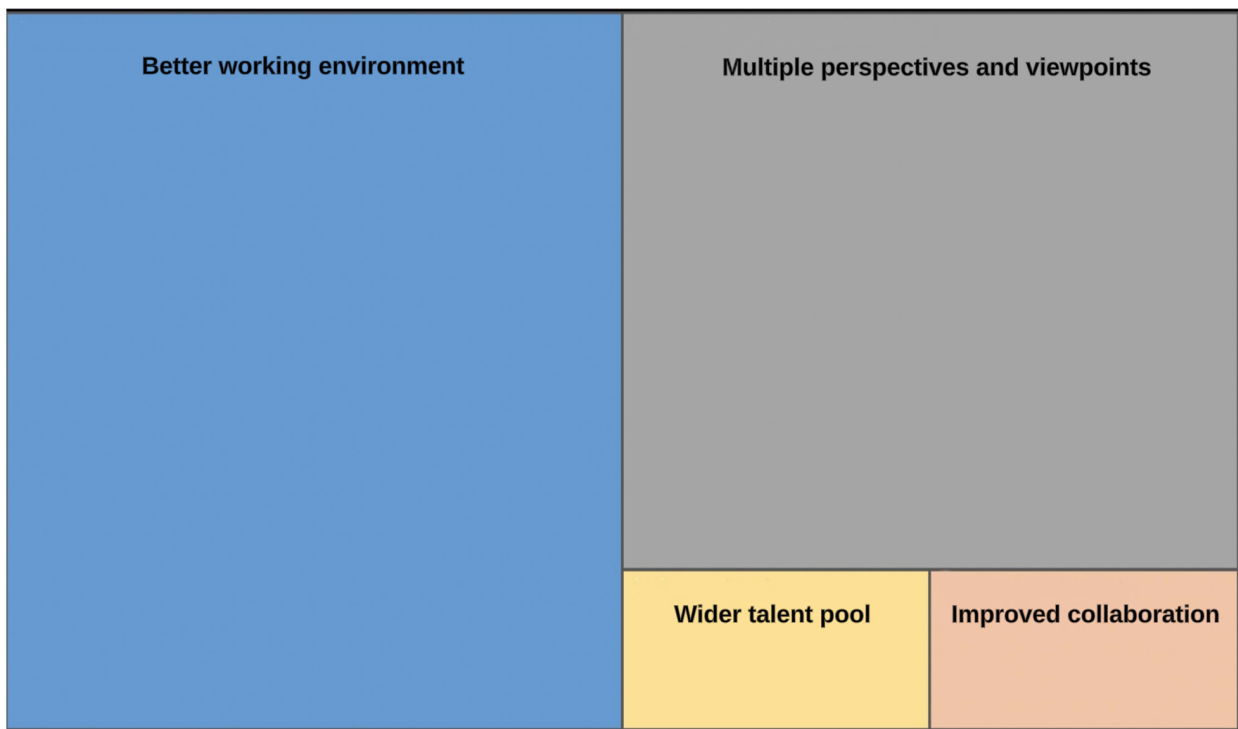


Figure 4.2: The effects of gender equality in cybersecurity

The effect with the second-highest ratio of responses is "multiple perspectives and viewpoints" with half of all respondents highlighting this as an advantageous. This effect addresses the reality that girls and boys are fundamentally different and bring distinct views to the table, resulting in new ideas and approaches. Respondent eleven had the following to say about it:

"In certain ways, girls think quite differently than guys. When I say that, I'm being really general. We have a different comprehension, a different way of perceiving a situational image than boys have. I believe that girls will be able to provide slightly different thoughts, ideas, and points of view that will be of immense value to our clients. It's not only about having females or guys; it's about having a diverse team where everyone can contribute fresh ideas depending on their gender, culture, upbringing, education, etc. If you are too equal, the consumer will not receive the value they may have gotten. You get far more out of a team if you have various people in it".

Several respondents pointed out, among other things, that females have a slightly different mindset to risk, tend to see more of the big picture, and see the psychology of information security rather than the technical way of thinking. All of which are important qualities for a cybersecurity professional. Additionally, as respondent 12 so eloquently put it:

"When a certain sort of individuals is collected together, it often becomes "group-think" or an echo chamber where the same thoughts are flung back and forth, which causes them to join and become more integrated in the organization. When there is diversity, these ideas are questioned to a larger level, which might lead to the ideas being processed and developed further. So, I feel that equality will lead to the company evolving and gaining a stronger foundation for decision-making that takes into account more factors.

People will produce the same results if they consistently think in the same manner, as the person in question indicates. This only comes to an end when different ideas and points of view are heard.

4.4 Summary

According to the findings of the interviews, there are numerous barriers that prevent women from pursuing a career in cybersecurity. The recurring themes of the barriers correspond to the barriers identified in the literature, demonstrating how they are still relevant today. The respondents were also asked how these barriers could be overcome, which resulted in a list of the top five measures to attract and retain women in cybersecurity. These measures included, showing possibilities and raising awareness, overcoming stereotypes and misconceptions, role models, flexibility, and taking inspiration from other male dominated professions, of which showing possibilities was the measure with the highest ratio of answers. Because the measure "showing possibilities" is the most frequently suggested, it will be examined in greater depth in the following chapter.

Furthermore, this chapter continued with an assessment of the value of female cybersecurity professionals in organizations. The respondents addressed the question, "How might the increased representation of female cybersecurity professionals contribute to an organization?", where the most commonly proposed effect was an improved working environment, followed by multiple perspectives and viewpoints, wider talent pool, and improved collaboration. And, based on the findings, one might conclude that the majority of respondents support increased gender diversity in the workplace.

Chapter 5

Discussion

The purpose of this study has been to examine how the cybersecurity industry might benefit from, as well as entice and retain, female cybersecurity professionals. By narrowing it down to a female perspective, the objective of this exploratory study have been to identify the several barriers keeping women from pursuing a career in this profession, and to develop a set of recommendations as to how to overcome these. Meanwhile, the goals were to understand how the barriers preventing women from cybersecurity are connected, and to identify a way of turning this around based on the proposed measures from the interview respondents. The following chapter discusses the literary findings from chapter two to the empirical findings obtained through our qualitative research, where the purpose is to answers our research questions:

- RQ: *"How can the cybersecurity industry entice and retain woman?"*
- SRQ: *"How might the increased representation of female cybersecurity professionals contribute to an organization?"*

5.1 Analysis of Findings

Looking at the data, both the literature and the findings from the interviews identified barriers and reasons why women are underrepresented in the cybersecurity industry. Based on the identified barriers, interview respondents recommended a variety of strategies to overcome these barriers. "Showing possibilities" had the largest ratio of responses, therefore we chose to focus primarily on this metric. One major reason for this is that we discovered a connection from the absence of showing possibilities to the other barriers identified, as well as seeing how showing possibilities corresponds with the additional measures recommended. The findings have implications for further research and practice, which will be examined and explained in the sections below.

5.1.1 Theoretical Implications of the Metric "Showing Possibilities"

We made the decision to create a causal model that would demonstrate how many occurrences affect one another in order to gain an understanding of the reasons why girls do not pursue a career within cybersecurity. This is particularly crucial as we need to map out the variety of barriers that prohibit women from viewing a career in cybersecurity as an opportunity before we can think about potential solutions to this issue. In this instance, a causal model is perfectly suited since it closes the gap in correlational research by identifying the causes for the relationships in variables. We may create methods for resolving issues by knowing how different variables influence the outcome. Given the capacity to generate predictions that causal research provides, the insights can be used for purposes other than understanding cause and effect. It may produce future ideas that are related to or include the variables from this research, as we shed light on such a complex issue.

The Vicious Cycle of not Showing Possibilities

The findings derived from the reviewed literature and the qualitative data formed the vicious cycle of not showing possibilities depicted in Figure 5.1. The model addresses the metric "showing possibilities and raising awareness," which received the most feedback from the interviews, and is based on the assumption that stereotypes, disinformation, discrimination, lack of role models and insufficient information about the possibilities lead to low self-efficacy, which in turn contribute to girls' low interest in the subject. All of this results from a little degree of information about the field of cybersecurity as a whole.

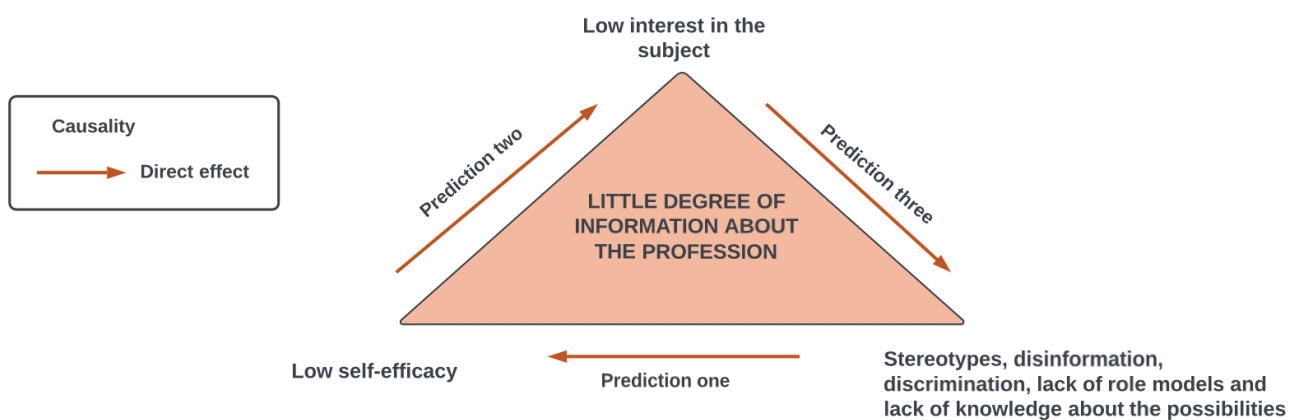


Figure 5.1: The vicious cycle of not showing possibilities

Albert Bandura's "Social Cognitive Career Theory" served as an inspiration for the idea in which a person's feeling of self-efficacy affects career-related decisions (Gladstone and Cimpian, 2021). The theory's core premise is that we are motivated to engage in activities we think we are able to succeed in (Gladstone and Cimpian, 2021). According to the literature and the interviews, girls struggle more than males do with self-efficacy and have self-doubt, which leads to their decision not to pursue careers in the cybersecurity industry. The fact that females are more likely to have doubts about their own abilities and skills leads to them being unable to envisage themselves in the sector, resulting in decreased interest in the profession. In other words, there is a bigger likelihood that interests won't emerge when females believe they are not skilled or competent enough for the cybersecurity industry and anticipate bad outcomes. The barriers that were identified in the reviewed literature turn out to be in line with those that interview respondents also believed prevented girls from

selecting a profession in cybersecurity. They have thus been maintained in our prediction that barriers like stereotypes, disinformation, discrimination, a lack of role models, and a limited understanding of the possibilities in the cybersecurity profession are all thought to contribute to women's low self-efficacy. Our prediction stems from the fact that these barriers, each in their own manner, deter girls from pursuing professions in cybersecurity by making them question their own ability.

Stereotypes and disinformation that women are "less competent" in STEM subjects or that computer security is considered to be a "man's job" are detrimental to women since they instill girls a sense that they don't belong in the industry, which leads to poor self-efficacy. As a consequence of these stereotypes, girls are less interested in these subjects than their male peers. This is related to discrimination as well, as it is claimed in the literature that educators and parents undervalue women's mathematical abilities and assume boys have a better foundation for success in the STEM professions, even if this is untrue. Parents' and teachers' gender prejudices may lead women to believe they are unsuitable for careers in cybersecurity, while the truth is quite otherwise according to the reviewed literature and the interviewees.

The model additionally demonstrates that girls' low self-efficacy might come from the lack of role models in the industry. A crucial source of self-efficacy, according to Social Cognitive Theory, is seeing a related role model succeed at a similar task (Gladstone and Cimpian, 2021). This is connected in that sense that seeing others complete a task successfully may lead one into thinking that they can complete the task as well. The shortage of female role models in the cybersecurity field contributes to girls having no one to look up to, admire, or identify with, making it more likely that women would reject cybersecurity as a career option. The presence of female role models in cybersecurity can boost girls' implicit identification with the subject while eliminating gendered preconceptions.

Lastly, as the model above suggests, the final barrier that might lead to girls' low self-efficacy is lack of knowledge about the possibilities. The impression that one must be technically inclined or work as a programmer to be in this industry is a deterrent for many women and is what drives them away, according to both the literature and the respondents. Women who hold this belief have a harder time visualizing themselves working in the profession, which affects their self-efficacy. The reality is that the cybersecurity sector needs a wide variety of people, and that cyber work is as much about impact on people as it is about technology (Weingarten and Garcia, 2015). It's critical to let women know that coding expertise is not a requirement for success in the cybersecurity industry. There are numerous other skills that would be valued, and each of them would help to close the current skills gap.

The Virtuous Cycle of Showing Possibilities

In terms of "the vicious cycle of not showing possibilities", our aim is to turn this into something virtuous. Looking at the identified solutions and measures to remove the barriers preventing women from entering cybersecurity, the literature and qualitative data had many similarities, but also some important disparities. The literature emphasizes the significance of parents and educators treating children more gender neutrally and encouraging both male and female students to pursue interests such as mathematics and technology. Furthermore, the interviewees encouraged women to pursue a career in the industry if they were interested, and to use the fact that women are a minority in this field to their advantage. However, the importance of showing the possibilities of cybersecurity and increasing awareness of its profession was shared by both the literature and interview respondents.

The causal model of the virtuous cycle of showing possibilities is depicted in Figure 5.2. The model is built around the main measure "showing possibilities and raising awareness", which is correlated to the other four proposed metrics analyzed in chapter 4.2. "Showing possibilities and raising awareness" was the proposed measure with the highest ratio of answers. However, by incorporating the other four measures as well, we are increasing our knowledge of cybersecurity and raising awareness of this profession.

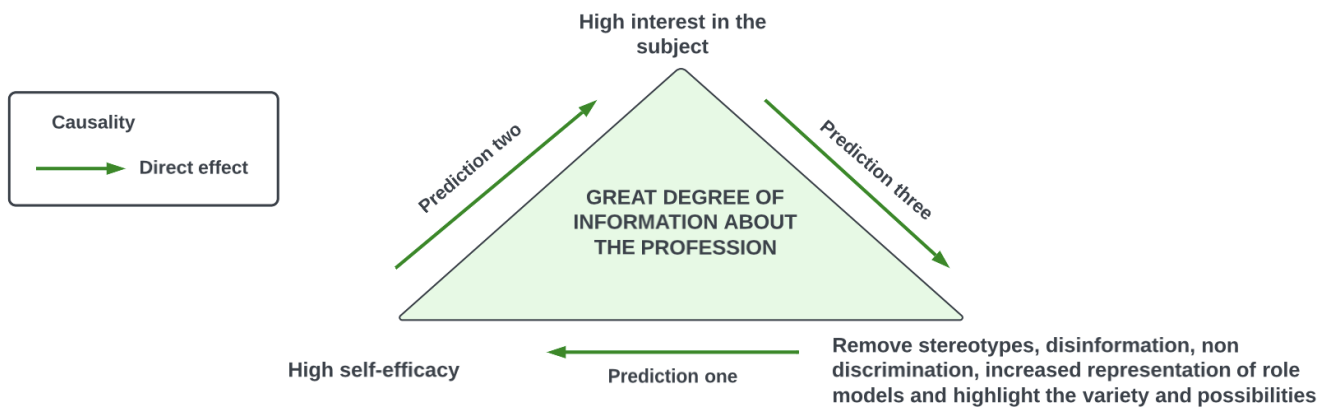


Figure 5.2: The virtuous cycle of showing possibilities.

According to the causal model depicted in Figure 5.2, the assumption is that by implementing efforts to reduce the barriers that prevent women from entering cybersecurity, we will have a great degree of information about the profession. As a result, our prediction is that stereotypes, disinformation, and discrimination will be reduced. Thus, will the representation of female role models increase, as will the variety and possibilities of cybersecurity. As previously stated, this is all related to women’s self-efficacy. Prediction one includes women acquiring higher self-efficacy in cybersecurity as these barriers dissolve. The model additionally demonstrates the correlation between high self-efficacy and high interest in cybersecurity. When you have confidence in your abilities and a sense of expertise, this leads to a greater degree of interest in the field. Increased interest in the subject will also help to remove misconceptions, misinformation, and discrimination in cybersecurity, as well as increase the representation of female role models as prediction three shows. As the literature established, both education and exposure of cybersecurity is important metrics for attracting women into the profession. And according to Weingarten and Garcia (2015), lack of knowledge about cybersecurity is the reason for the gender gap. Thus, the causality model illustrates how we can attract and entice more women in cybersecurity by creating a great degree of information about cybersecurity.

5.1.2 Implications for Practise

Based on the aforementioned findings, we have created a series of recommendations targeted at the educational and industry sector that can help to strengthen the metric "showing possibilities and raising awareness" and remove the numerous barriers that occur in the "vicious cycle" in Figure 5.1. Even though some of these recommendations are explicitly directed towards women, they can all apply to both men and women. However, because they now make up a minor portion of the cybersecurity industry, attention is given to women. In order to effect long-term change, the recommendations have been divided into two primary sectors with the potential for change.

Recommendations Aimed at Educational Sector

The recommendations that follow are focused at the educational sector, as the findings identified changes to this sector as being necessary for improving the participation and perception of women in cybersecurity.

- *Reframing cybersecurity as an industry and as a term*
There is widespread recognition that the general perception of the cybersecurity industry is a major contributor to the shortage of women in the field. Raising awareness of the industry and portraying it accurately and positively is essential for growing the number of women in cybersecurity. To counterbalance views of excessive requirements and gender disparities, new narratives emphasizing the attractiveness and utility of cybersecurity are required.
- *Early awareness raising*
The goal of early awareness training is to raise awareness of cybersecurity as early as feasible and to promote it as a career option. This was a metric that came up repeatedly in the interviews, yet respondents had varying opinions on when it should be implemented. However, the majority of participants thought it should happen before university, preferably before upper secondary school, because this is when most people have decided what they want to study. One respondent mentioned that if we want to influence children, we need to talk about it in ways they can understand. The notion of reaching out to children is intriguing, as the theory explains how early gender norms are formed. According to Olaiya and Petronella (2011), children start developing stereotypes as young as three and five years old. As we have seen, stereotypes help prevent girls from cybersecurity, and it is therefore important to counteract stereotypes as early as possible. And according to the theory, this should happen at kindergarten age.
- *Teaching IT and cybersecurity through games*
In terms of talking about cybersecurity in ways children can understand, this recommendation seeks to reach out to different age groups through various sorts of games in order to educate them about IT and cybersecurity. One example highlighted in the interviews was designing some types of games with VR to target the youngest audience. Competitions and tasks like "capture the flag" are other examples of existing methods that should be promoted further in the educational sector. These ideas are assisting in making IT and cybersecurity more apparent and demystifying what it entails.
- *Key influencers*
This recommendation requires the education of key influencers, who could range from family to teachers, learning assistants, and professors. According to the literature, "the lack of role models or key influencers is arguably the most important reason why women are underrepresented in cybersecurity," which stems from a lack of female representation both in the educational sector as cybersecurity teachers and professors as well as a lack of female cybersecurity professionals. It also includes the lack of knowledge both primary educators and family have on the subject. Furthermore, several of the respondents had parents who worked in STEM fields, and it was these respondents who received familial encouragement to pursue a career in cybersecurity. This is an example of the power of influence family and other key influencers has, which is why the showing the possibilities and raising awareness of cybersecurity should be addressed at everyone, not only young girls, in order to expand female representation in the sector.

- *Competency requirement*

This recommendation attempts to incorporate cybersecurity into the upper secondary school curriculum by incorporating it as a competency requirement inside an existing subject. Several of the respondents identified upper secondary school as a key factor to the gender gap in technical skill development between men and women in the cybersecurity field. Respondent thirteen even suggested making cybersecurity a mandatory subject, however by integrating a competency requirement, less needs to be modified in the curriculum, and thus change may occur more quickly. This also corresponds to the literature in that it indicates that education is the key to closing the gender gap in the cybersecurity industry as well as removing the accompanying misconceptions and stereotypes.

- *Scholarship and internship programs*

There are various initiatives that can be implemented to encourage female students to pursue careers in cybersecurity. Scholarships for students and internship opportunities at various organizations can be used to promote the cybersecurity profession. By providing cybersecurity scholarships, financial barriers are solved while also promoting the subject. Internships, however, operate to the extent that students have the opportunity to work with the subject at an organization. This provides students with insight into the field, allowing them to obtain experience that could result in greater opportunities for future employment in the cybersecurity industry. This helps to promote and create knowledge about cybersecurity professions.

- *Workshops*

Conducting workshops is a recommendation we developed entirely for the purpose of showing possibilities and raising awareness of cybersecurity. The majority of respondents suggested that we demonstrate what cybersecurity is all about and present it in a way that allows people to feel more connected to the subject. While workshops are excellent for introducing cybersecurity and expanding knowledge, research shows that this also assist enhance women's confidence and self-efficacy (Rowland et al., 2018). Providing girls with informal, autonomous educational chances, like workshops, can help them gain confidence and interest for this field (Rowland et al., 2018).

Recommendations Aimed at Cybersecurity Industry Sector

The following recommendations concentrate on how organizations and businesses can attract and retain female cybersecurity professionals, with a particular emphasis on employee retention.

- *Use gender-neutral language and illustrations*

To avoid disinformation and stereotypes, such as the view that women are unsuitable for studying and working in cybersecurity, we recommend businesses and organizations to be mindful on how they speak about and depict the profession. When displaying and describing a career field, one should be conscious of how words and images are used because they might indirectly convey information about what a profession can be like and who is qualified for it. This is especially true for the cybersecurity industry, which both the literature and the respondents agree has an image problem. Therefore, we advise businesses and organizations to adopt gender-neutral language and illustrations so that cybersecurity does not appear repulsive to women.

- *Promote flexibility*

Women considering a career in cybersecurity may encounter challenges due to the

industry's lack of flexibility. Multiple initiatives could entice more women to work in cybersecurity and help them succeed in the field. One development is the increase in remote work, which may make the sector more adaptable and accessible to women. Along with remote work, it was also noted that work hours should be made more flexible to better meet the demands of the employee. Some of the respondents offered this as an attempt to recruiting more girls into the field. This flexibility policy may give girls the notion that they do not need to give up anything in order to grow in their careers, as they do not need to balance work and family obligations.

- *Visibilize role models and ambassadors*

This recommendation focuses on the importance of having visible role models and ambassadors that girls can look up to and identify with. The slogan "*you can't be what you can't see*" sums this up nicely (Gladstone and Cimpian, 2021). Once more, this relates to Bandura's social cognitive theory of self-efficacy, an individual's belief of their ability for learning and success in a given domain (Gladstone and Cimpian, 2021). As previously stated by the literature and the respondents, women exhibit poorer self-efficacy than males in terms of their ability to succeed in the cybersecurity profession. By serving as a successful example, role models can help to improve a student's motivation. Seeing other girls thrive in the profession might instill a sense of worth and belonging in other girls. Thus, women in cybersecurity need to take ownership of their role as ambassadors and encourage young women to pursue careers in the industry. Organizations and businesses can play a significant role in removing the myth that cybersecurity is exclusively a man's field by introducing female role models as guest speakers at schools. This will help girls connect with female role models when making decisions about their future educational and professional paths.

- *Cross industry initiatives for women*

This recommendation is about raising awareness among women regarding the numerous career options in cybersecurity through various cross-industry initiatives in order to dispel the misinformation that this is not a friendly field for women. Through these initiatives, women have the chance to network and connect with one another, which can help them grow in their careers.

- *Mentorship and training program*

In addition to encouraging more women to enter the field of cybersecurity, it's crucial to support and retain the women who are already in the industry. For organizations and firms trying to keep their female cybersecurity employees, mentorships and training programs can be effective strategies. Giving new graduates access to a unique resource, such as a female colleague who is currently in the field and has gone through similar experiences, may be immensely inspiring. Women can gain a lot from working with an experienced mentor in the cybersecurity sector who can provide them advice and guidance on how to succeed and grow in a male-dominated field. Since girls are more prone than men to experience imposter syndrome, mentorship, along with training programs, can help women to develop confidence and a sense of mastery.

- *Foster a welcoming & inclusive community*

This recommendation urges organizations and businesses to take steps to ensure that the workplace supports diversity, inclusiveness, and a pleasant work culture. Positively, this tendency has become more prevalent in the recent years as more businesses and organizations start recognizing the value of diversity. Nevertheless, as some respondents pointed out, there are still some workplaces where discrimination occurs, as well as the so-called "*boys' club*". For women to dare to enter a predominantly male-dominated area such as cybersecurity, there must be a shift in attitude in which discrimination and harassment is not tolerated.

The Overall Model of the Recommendations to Entice and Retain Women

In summary, the recommendations in Figure 5.3 are our proposals for enticing and retaining women in the cybersecurity industry. They refer to long-term initiatives that can be performed at both educational and organizational levels to increase the female representation.

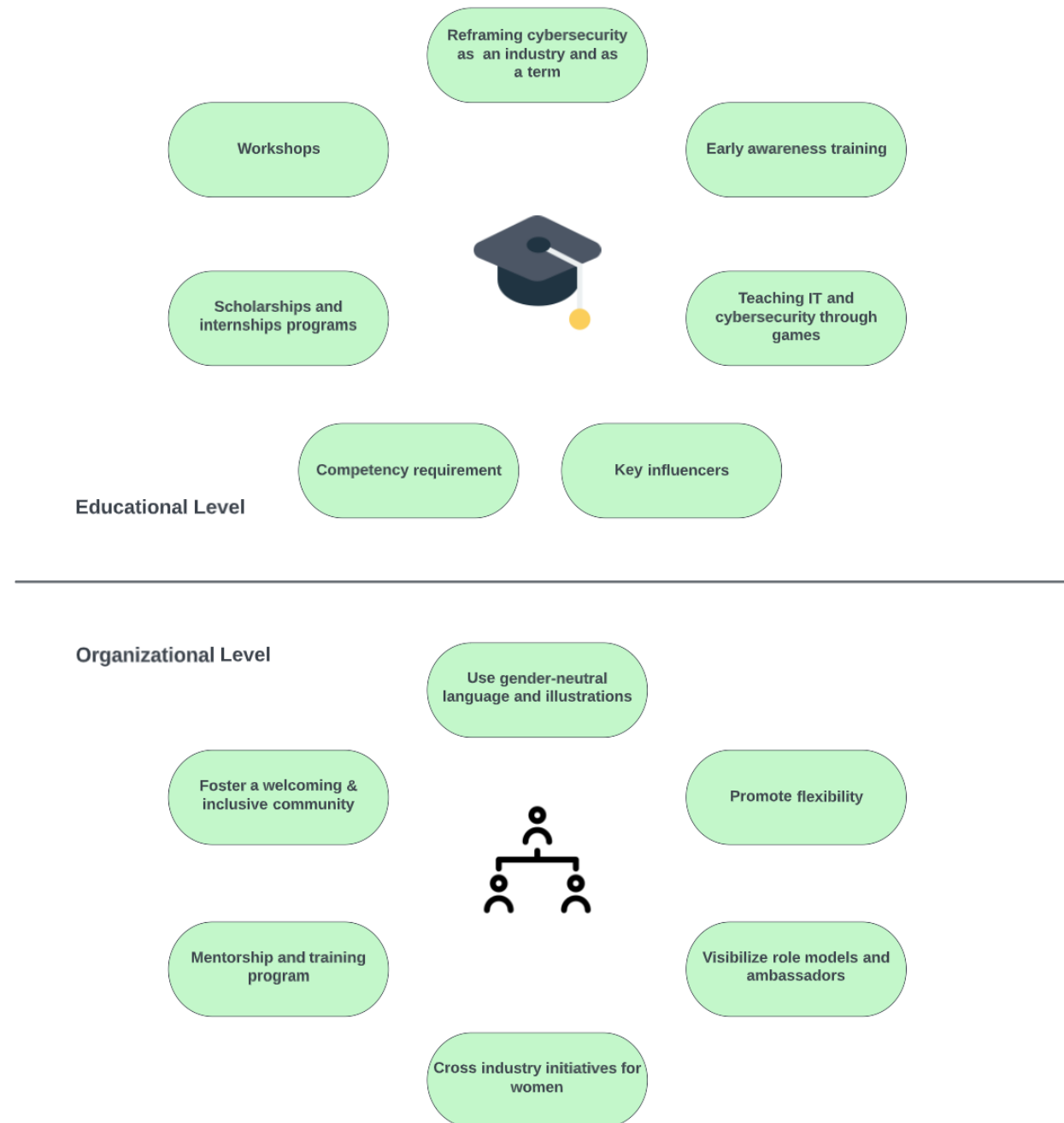


Figure 5.3: The recommendation's overarching model

5.1.3 The Effects of Female Cybersecurity Professionals in the Industry

In terms of the sub-research question "How might the increased representation of female cybersecurity professionals contribute to an organization?", the results reveal that the literature findings agree well with the outcomes of the interviews. The respondents concur with the literature and recognize the need of having female cybersecurity professionals in organizations. This gives validity to the assertion that more female cybersecurity professionals are urgently needed in the field. Based on our findings, we identified the beneficial advantages listed below as the reasons why organizations should invest more in a diversified workplace:

- Wider talent pool
- Strengthened customer orientation
- Boosted satisfaction among employees
- Improved decision-making
- Improved company image
- More profitable business

Fortunately, more organizations are beginning to recognize the benefits of a diverse work environment, and we are seeing an increase in the number of workplaces that have a minimum criteria for how many female employees they would like to employ. However, based on our data, there is still a long way to go. According to our respondents, the average percentage of female cybersecurity professionals in the organizations we interviewed is 22%, which is lower than the global average at 25% (Ventures, 2022). This clearly demonstrates the necessity of taking steps to enhance this percentage and even out the gender imbalance. Recruiting more female workers, regardless of industry, will benefit both the business and the employers. As a result, attracting and retaining female cybersecurity professionals isn't just the ethical thing to do; it's also good business.

Chapter 6

Conclusions

This exploratory study aimed to find out more about the gender gap in the cybersecurity sector, the need for fresh ideas, and how to inspire and provide solutions to support more women in choosing this career path. Based on this, an analysis of the chosen topic was conducted, resulting in a causal model that seeks to explain the numerous barriers that females encounter in the cybersecurity industry and how they connect to a person's self-efficacy and interests. The findings demonstrate that stereotypes, disinformation, discrimination, a lack of role models and a lack of knowledge about possibilities are among the barriers contributing to the challenges that women face today in the field of cybersecurity. Therefore, in order to increase the number of women working in cybersecurity today, these barriers must be removed. Subsequently, with the potential for change in attracting and retaining more female cybersecurity professionals, a set of recommendations addressing both the educational sector and the cybersecurity industry were developed. As a result, it is necessary for the educational sector to redefine cybersecurity as an industry and as a term, increase early awareness, communicate the subject in a way that all age groups can understand, educate key influencers, possibly make it a prerequisite for competency, provide scholarships and internship opportunities, and finally hold workshops to increase the participation of women in the field. Whereas, recommendations for the cybersecurity industry sector include using gender-neutral language and imagery, promoting greater flexibility, visualizing role models and ambassadors, providing cross-industry initiatives for women, offering mentorship and training programs, and lastly promoting a welcoming and inclusive community. The measures mentioned are all recommendations that might help to attain the goal of attracting and retaining more women in the sector. Additionally, our research suggests that greater participation of women in the workforce will have positive and competitive impacts, such as a larger talent pool, more employee satisfaction, better decision-making, an improved company image, and ultimately a more profitable business. The findings indicate that there is a compelling business justification for seeking more diverse representation.

6.1 Contribution to Theory and Industry

Our study contributes to advance gender equality in the cybersecurity industry by identifying the barriers that keep women out of the field and proposing long-term strategies that can be used to attract and retain more women. By introducing "The Vicious Cycle of Not Showing Possibilities," we obtain a greater understanding regarding how the numerous barriers are connected and hinder women from pursuing a profession in cybersecurity. To elaborate, we opted to create the causal model since it bridges the gap in correlational research by explaining the reasons for variable connections. Following, the causal model "The Virtuous Cycle of Showing Possibilities" expands on how the proposed measures can aid in the removal of the barriers, as well as demonstrating how much of an improved impact implementing specific measures can have. Furthermore, we identified research gaps from the findings to determine

what measure were missing to achieve a greater degree of gender equality in the industry. This resulted in a set of recommendations divided into what both the educational and organizational sector can do to increase the female representation of cybersecurity professionals.

For industry, our work will assist to attract and retain more women in the cybersecurity profession, as the recommendations we propose can be implemented not only by the educational sector, but also by the organizations themselves. Even organizations outside of the cybersecurity industry can make use of the recommendations, and gain input in how to attract more female employees as well as fostering a more diverse work environment. This study can thus be applied to a variety of male-dominated industries.

6.2 Limitations and Future Directions

The exclusion of the male viewpoint

This study only looks at the female perspective as they are the minority in cybersecurity. Thus, the male perspective was excluded. This aligned well with the study's scope, yet expanding the study to include the male perspective could have provided new feedback and ideas on how to proceed in order to eliminate gender inequalities. As our research shows, gender diversity improves organizational performance, therefore this would most certainly be beneficial for this study as well.

Insufficient sample size: too few respondents

During the interview process, we observed data saturation and were thus at the time pleased with the quantity of respondents interviewed. Although we achieved data saturation, it was not a given, and we can see in retrospect that more respondents would have improved the validation of the findings. We can remark that because we were looking for the perspective of a minority group, it is a small population to sample from, making it difficult to locate an adequate sample size.

Geographic constraints

Considering all of the interviews were conducted in Norway, the work is geographically constrained. Despite the fact that several of the organizations studied are internationally, we have focused on Norwegian work culture in relation to gender equality. This may limit our task because various cultures' perspectives on gender equality in cybersecurity may differ. As a result, we can see that expanding the study to cover a greater geographical area can increase the accuracy of the barriers and, as a result, the recommendations.

Validate the vicious and virtuous cycle.

Further research may examine the validity of our theoretical implication of the vicious and virtuous circle of the metric "showing possibilities". Although Albert Bandura's "*Social Cognitive Career Theory*" served as the foundation for this idea, a substantial portion of it is based on our predictions drawn from the findings of the reviewed literature and the responses from our interviewees. As a result, we are unable to confirm with certainty the validity and accuracy of this contribution because it has not been tested; however, both the theoretical underpinnings and the responses from our interviewees provide insight into the reasons why there are so few women in the profession and offer suggestions for how to change it.

Inclusion of the male perspective.

The inclusion of the male perspective might constitute another contribution to future research. It would have been intriguing to investigate whether men's thoughts and views on the subject at hand varied from those of women. Especially given that they constitute the

vast majority of the sector's workforce and might approach this differently. Therefore, in order to develop a comprehensive grasp of the situation, future research should consider the perspectives of both sides.

Using mix-methods research.

Mixed-methods research, which combines both qualitative and quantitative data, can improve a study by ensuring that the benefits of one form of data are balanced out by the flaws of the other. A survey might be used to create hypotheses based on the perspectives discovered through qualitative research, and then a quantitative technique could be used to evaluate them against a bigger sample. Any upcoming research can take this into consideration.

Appendix A

Interview Guide

1. Si litt om deg selv, nåværende stilling, bakgrunn som studier eller tidligere jobber.
 - (a) Hvorfor valgte du utdanningen du har?
 - (b) Når tid var første gang du ble informert om cybersikkerhet som en karrieremulighet?
 - (c) Ble du påvirket/inspirert av for eksempel venner, foresatte, familie medlemmer, mentorer, bekjente eller andre til å velge en karriere innenfor cybersikkerhet?
2. Hva gjorde at du endte opp i denne jobben?
 - (a) Var det et bevisst veivalg å havne i denne avdelingen?
3. Hvor mange kvinner jobber innenfor din avdeling?
 - (a) Hva er din tanke om denne prosentandelen?
4. Hva er din oppfatning av det generelle kjønns mangfoldet innenfor cybersikkerhet feltet?
 - (a) Hvorfor tror du det er slik innen cybersikkerhet?
5. Etter din mening, tror du kjønnslikestilling vil ha en påvirkning på arbeidsplassen?
 - (a) Hvordan vil likestilling positivt påvirke organisasjonen?
6. Hvordan tror du det ville sett ut dersom organisasjonens mål om kjønnslikestilling var møtt?
7. Hva tror du må til for at flere kvinner skal velge å studere og jobbe innen cybersikkerhet?
8. Hvordan vil du beskrive mulighetene for en kvinne innen cybersikkerhet i dag?
9. Hva ser du på som det største hinderet som må overvinnnes for at flere kvinner skal følge denne karriereveien?
10. Føler du at kvinner har mer å bevise i en bransje innenfor cybersikkerhet?
 - (a) Blir kvinner gitt lik anerkjennelse som sine mannlige kollegaer?
11. Var det noe som nesten fikk deg til å ombestemme deg angående cybersikkerhet sektoren?
12. Hva vil være ditt viktigste råd til kvinner som vurderer en karriere innenfor cybersikkerhet?

Til ledere:

1. Hva gjør dere for å tiltrekke og beholde kvinnelige ansatte hos dere?
 - (a) Gjøres det tiltak i ansettelsesprosessen for å utjevne organisasjonens kjønnsmangfold?
 - (b) Brukes det mange maskuline ord og overflod av tekniske ferdigheter i stillingsbeskrivelsene?

Eventuelle tilleggsspørsmål:

1. Har menn større sjanse for å lykkes i denne bransjen?
2. Har du opplevde du noe form for kjønnsstereotyper ved å velge cybersikkerhet?
3. Er det noen faktorer du tenker at vi ikke har spurt om og som burde vært med?

Appendix B

Consent Form

Are you interested in taking part in the research project

“The impact of Gender Equality In the Cybersecurity Sector”?

Purpose of the project

You are invited to participate in a research project where the main purpose is to address how the cybersecurity industry can entice and retain women. As women continue to be underrepresented in the cybersecurity industry, it is crucial to encourage more of them to pursue careers in this area. We will therefore identify the reasons that prevent women from pursuing careers in cyberspace and work to discover solutions. The research project is a master's thesis.

Which institution is responsible for the research project?

The faculty of Engineering and Science at University of Agder is responsible for the project.

Why are you being asked to participate?

In view of our research project, we want to gain different perspectives of people working within cybersecurity. We want to collaborate with major companies that are focused on cybersecurity in order to boost the study's academic value and weight.

What does participation involve for you?

The participation involves taking part of semi-structured interviews and questionnaires. The individuals' attitude and opinion regarding gender inequalities in the cybersecurity industry will be collected, as well as the companies' management of this issue. The information will be recorded electronically including video and audio. The interviews are estimated to last approximately 30 – 45 minutes.

Participation is voluntary

Participation in the project is voluntary. If you choose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be deleted. There will be no negative consequences for you if you choose not to participate or later decide to withdraw. It will not affect your relationship with your place of work.

Your personal privacy – how we will store and use your personal data

We will only use your personal data for the purpose(s) specified here and we will process your personal data in accordance with data protection legislation (the GDPR). Those who have access to the personal data is the project group and its supervisors. Measures that will be taken to ensure that unauthorized persons do not have access to the personal data are by anonymizing the participants' name. The list of names and the contact details will be stored separately from the rest of the collected data and the data will be stored on a cloud server which is locked away.

What will happen to your personal data at the end of the research project?

The planned end date of the project is December 31st, 2023. The personal data including digital recordings will be deleted at the end of the project.

Your rights

So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and

Figure B.1: NSD consent form

- send a complaint to the Norwegian Data Protection Authority regarding the processing of your personal data

However in this study, we will not collect your personal data. Both the company and the participant will be anonymized.

What gives us the right to process your personal data?

We will process your personal data based on your consent.

Based on an agreement with the University of Agder and the of Engineering and Science, Data Protection Services has assessed that the processing of personal data in this project meets requirements in data protection legislation.

Where can I find out more?

If you have questions about the project, or want to exercise your rights, contact:

- Faculty of Engineering and Science at UiA via Ragnhild Sofie Ertzeid Toft and Tuva Cecilie Eikaas, by email: (rstof18@uia.no) or (tuvace18@uia.no).
- The project's supervisors: Jaziar Radianti and Terje Gjøsæter.
- Our Data Protection Officer: University of Agder.

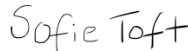
If you have questions about how data protection has been assessed in this project, contact:

- Data Protection Services, by email: (personvermtjenester@sikt.no) or by telephone: +47 53 21 15 00.

Yours sincerely,

Terje Gjøsæter
Project Leader
(Researcher/supervisor)

Student (if applicable)



Consent form

I have received and understood information about the project “The impact of gender equality in the cybersecurity sector” and have been given the opportunity to ask questions. I give consent:

- to participate in an interview

I give consent for my personal data to be processed until the end of the project.

(Signed by participant, date)

Figure B.2: NSD consent form

Bibliography

- Al-Alawi, A.I., Al-Khaja, N.A., Mehrotra, A.A., 2023. Decrypting cybersecurity's gender gap. *Journal of International Women's Studies* 25. URL: <https://vc.bridgew.edu/cgi/viewcontent.cgi?article=3048&context=jiws>.
- Alshenqeeti, H., 2014. Interviewing as a data collection method: A critical review. 1 3. doi:10.5430/elr.v3n1p39.
- Amo, L., 2016. Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. *IEEE Security & Privacy* 14. URL: <https://ieeexplore.ieee.org/document/7397723>, doi:10.1109/MSP.2016.12.
- Chan, R.C., 2022. A social cognitive perspective on gender disparities in self-efficacy, interest, and aspirations in science, technology, engineering, and mathematics (stem): the influence of cultural and gender norms. *International Journal of STEM Education* URL: <https://stemeducationjournal.springeropen.com/articles/10.1186/s40594-022-00352-0#citeas>, doi:<https://doi.org/10.1186/s40594-022-00352-0>.
- Cheryan, S., Master, A., Meltzoff, A.N., 2015. Cultural stereotypes as gatekeepers: increasing girls' interest in computer science and engineering by diversifying stereotypes. *Frontiers in Psychology* 6. URL: <https://www.frontiersin.org/articles/10.3389/fpsyg.2015.00049>, doi:10.3389/fpsyg.2015.00049.
- Chompunuch, S., Ribiere, V., Chanal, V., 2019. Exploring and modeling the concept of team creativity.
- Cobb, M.J., 2018. Plugging the skills gap: the vital role that women should play in cyber-security. *Computer Fraud & Security* 2018. URL: <https://www.sciencedirect.com/science/article/pii/S1361372318300046>, doi:[https://doi.org/10.1016/S1361-3723\(18\)30004-6](https://doi.org/10.1016/S1361-3723(18)30004-6).
- Cooper, C., Booth, A., Varley-Campbell, J., Britten, N., Garside, R., 2018. Defining the process to literature searching in systematic reviews: a literature review of guidance and supporting studies. *BMC Medical Research Methodology* 18. URL: <https://bmcmmedresmethodol.biomedcentral.com/articles/10.1186/s12874-018-0545-3>, doi:<https://doi.org/10.1186/s12874-018-0545-3>.
- Cresswell, J., 2008. The Selection of a Research Design the Three Types of Designs. URL: https://www.sagepub.com/sites/default/files/upm-binaries/22780_Chapter_1.pdf.
- Das, S., 2020. Conceptualizing the Experiences of Women's Career Development in Cybersecurity: A Narrative Study. Ph.D. thesis. [Doctoral dissertation]. University of Georgia. Doctor of Philosophy (PHD). URL: <https://esploro.libs.uga.edu/esploro/outputs/9949366050502959>.
- Denzin, N.K., Lincoln, Y.S., 2008. *Strategies of Qualitative Inquiry*. SAGE.
- Fai, C.M., Goh, B., 2021. *Introduction to cyber forensic psychology*. World Scientific.

- Frost and Sullivan, 2017. The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Technical Report. ISC. URL: <https://www.isc2.org/-/media/Files/Research/ISC2-Women-in-Cybersecurity-2017.ashx?la=en&hash=FA78E4BDA2F858A0D3CFAC75AF9E789369A0BC8D>.
- Giboney, J., McDonald, J., Balzotti, J., Hansen, D., Winters, D., Bonsignore, E., 2021. Increasing cybersecurity career interest through playable case studies. *TechTrends* 65, 496–510. doi:10.1007/s11528-021-00585-w.
- Gladstone, J., Cimpian, A., 2021. Which role models are effective for which students? a systematic review and four recommendations for maximizing the effectiveness of role models in stem. *IJ STEM* 8. doi:<https://doi.org/10.1186/s40594-021-00315-x>.
- Gouett, M., 2021. Furthering Gender Equality Through Gender Bonds. Technical Report. International Institute for Sustainable Development (IISD). URL: <http://www.jstor.org/stable/resrep30865>.
- Griffin, C., 2004. The advantages and limitations of qualitative research in psychology and education. *Scientific Annals of the Psychological Society of Northern Greece* 2, 3–15. URL: https://www.researchgate.net/publication/310480387_The_advantages_and_limitations_of_qualitative_research_in_psychology_and_education.
- Harrell, M.C., Bradley, M.A., 2009. Data Collection Methods. Semi-Structured Interviews and Focus Groups. Technical Report. The RAND Corporation. URL: <https://apps.dtic.mil/sti/pdfs/ADA512853.pdf>.
- Hennink, M., Hutter, I., Bailey, A., 2020. Qualitative Research Methods. Social research methods series, Sage.
- Herring, C., 2017. Is diversity still a good thing? *American Sociological Review* 82, 868–877. URL: <http://www.jstor.org/stable/26426360>.
- Hoteit, L., 2022. Empowering women can help fix the cybersecurity staff shortage URL: <https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/>.
- Hunt, V., Layton, D., Prince, S., 2015. Diversity Matters. Technical Report. McKinsey Company. URL: <https://www.insurance.ca.gov/diversity/41-ISDGBD/GBDEExternal/upload/McKinseyDivmatters-201501.pdf>.
- Identity Theft, 2023. Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises. Technical Report. Identity Theft Resource Center. URL: <https://www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/>.
- Insights, F.B., 2022. Cyber Security Market Overview by Size, Growth & Trends. Technical Report. Fortune Business Insights. URL: <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>.
- ISC, 2022. ISC 2 Cybersecurity workforce study. Technical Report. ISC 2. URL: <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>.
- Jacobsen, D.I., 2015. Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. Cappelen Damm Akademisk.
- Kallio, H., Pietilä, A.M., Johnson, M., Kangasniemi, M., 2016. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *12* 72, 2954–2965. doi:<https://doi.org/10.1111/jan.13031>.

- Kaspersky, 2018. Beyond 11%: A study into why women is not entering cybersecurity. Technical Report. Kaspersky Lab. URL: <https://www.agec.org.au/wp-content/uploads/2018/09/Beyond-11-A-study-into-Why-Women-are-not-Entering-Cybersecurity-2017.pdf>.
- Khan, J.A., Rehman, I.U., Khan, Y.H., Khan, I.J., Rashid, S., 2015. Comparison of requirement prioritization techniques to find best prioritization technique. *International Journal of Modern Education and Computer Science* 7, 53–59. doi:10.5815/ijmecs.2015.11.06.
- Kitchenham, B., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering. Keele, UK, Keele Univ. URL: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.
- Lhammer, S., Hagman, L., 2021. Investigating Gender Disparity within Cyber Security. Ph.D. thesis. KTH Royal Institute of Technology. URL: <https://www.diva-portal.org/smash/get/diva2:1602714/FULLTEXT01.pdf>.
- Lingelbach, K.K., 2018. Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field. Ph.D. thesis. [Doctoral dissertation]. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. URL: https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2058&context=gscis_etd.
- Lune, H., Berg, B.L., 2017. *Qualitative Research Methods for the Social Science*. Pearson Education Limited.
- Myers, M.D., Newman, M., 2007. The qualitative interview in is research: Examining the craft. *Information and Organization* 17, 2–26. URL: <https://www.sciencedirect.com/science/article/pii/S1471772706000352>, doi:<https://doi.org/10.1016/j.infoandorg.2006.11.001>.
- National Cyber Security Center, n.d. What is cyber security? URL: <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security>.
- National Science Foundation (NSF), 1997. Analyzing qualitative data. URL: https://www.nsf.gov/pubs/1997/nsf97153/chap_4.htm.
- Oates, B.J., 2005. *Researching Information Systems and Computing*. SAGE Publications Inc.
- Olaiya, A.E., Petronella, C.A., 2011. Why does gender matter? counteracting stereotypes with young children. *Dimensions of Early Childhood* 39. URL: https://www.edu-links.org/sites/default/files/media/file/Why_Does_Gender_Matter_Counteracting_Stereotypes_With_Young_Children_Olaiya_E_Aina_and_Petronella_A_Cameron.pdf.
- Patticrew, M., Roberts, H., 2006. *Systematic reviews in the social sciences: A practical guide*. Blackwell publisher.
- Peacock, D., Irons, A., 2017. Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International journal of gender, science and technology* 9, 25–44. URL: <https://genderandset.open.ac.uk/index.php/genderandset/article/view/449>.
- Pifer, C.L., 2017. Cybersecurity Workforce Alert: Women’s Perspectives on Factors Influencing Female Interest. Ph.D. thesis. [Thesis or dissertation]. Frostburg State University ProQuest Dissertations Publishing. URL: <https://www.proquest.com/openview/b50bdf21e3b06df1fe163ed58bb13b28/1?pq-origsite=gscholar&cbl=18750>.

- Rowland, P., Podhradsky, A., Plucker, S., 2018. Cybher: A method for empowering, motivating, educating and anchoring girls to a cybersecurity career path. doi:10.24251/HICSS.2018.470.
- Sakellariou, c., Fang, Z., 2021. Self-efficacy and interest in stem subjects as predictors of the stem gender gap in the us: The role of unobserved heterogeneity. *International Journal of Educational Research* 109. URL: <https://www.sciencedirect.com/science/article/pii/S0883035521000902>, doi:<https://doi.org/10.1016/j.ijer.2021.101821>.
- Sarker, S., Xiao, X., Beaulieu, T., Lee, A.S., 2018. Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *Journal of the Association for Information Systems* 19, 761–763. URL: <https://aisel.aisnet.org/jais/vol19/iss8/1>.
- Sikt, 2023. Om sikt – kunnskapssektorens tenesteleverandør. URL: <https://sikt.no/tjenester/personverntjenester-forskning>.
- Simplilearn, 2023. It security roles and responsibilities of cyber security professionals. URL: <https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article>.
- Skills4, 2023. What is gender diversity? URL: <https://skills4training.org/what-is-gender-diversity/>.
- Snyder, H., 2019. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research* 104, 333–339. URL: <https://www.sciencedirect.com/science/article/pii/S0148296319304564>, doi:<https://doi.org/10.1016/j.jbusres.2019.07.039>.
- Stuckey, H., 2013. Three types of interviews: Qualitative research methods in social health. *Journal of Social Health and Diabetes* 1, 56. doi:10.4103/2321-0656.115294.
- Tellhed, U., Bäckström, M., Björklund, F., 2017. Will i fit in and do well? the importance of social belongingness and self-efficacy for explaining gender differences in interest in stem and heed majors. *Sex Roles A Journal of Research* URL: <https://link.springer.com/article/10.1007/s11199-016-0694-y#citeas>, doi:<https://doi.org/10.1007/s11199-016-0694-y>.
- Turban, S., Wu, D., Zhang, L., 2019. Research: When gender diversity makes firms more productive URL: <https://www.agec.org.au/wp-content/uploads/2021/10/2019-HBR-research-when-gender-diversity-makes-firms-more-productive-hbr2019.pdf>.
- UNICEF, 2017. Glossary of terms and concepts. URL: <https://www.unicef.org/rosa/media/1761/file/Gender>.
- U.S. Department of Education, 2021. Science, technology, engineering, and math, including computer science. URL: <https://www.ed.gov/stem>.
- Ventures, C., 2022. Women in cybersecurity 2022 report. URL: <https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf>.
- Wang, M.T., Degol, J.L., 2017. Gender gap in science, technology, engineering, and mathematics (stem): Current knowledge, implications for practice, policy, and future directions. *Educational Psychology Review* URL: <https://link.springer.com/article/10.1007/s10648-015-9355-x#citeas>, doi:<https://doi.org/10.1007/s10648-015-9355-x>.

- Weingarten, E., Garcia, M., 2015. Decrypting cybersecurity's gender gap. *New America*
URL: <https://www.jstor.org/stable/resrep10470>.
- Willis-Ford, C., 2018. The perceived impact of barriers to retention on women in cybersecurity URL: https://www.researchgate.net/publication/329754528_THE_PERCEIVED_IMPACT_OF_BARRIERS_TO_RETENTION_ON_WOMEN_IN_CYBERSECURITY, doi:10.13140/RG.2.2.13275.62244.
- Women, U., 2022. In focus: Sustainable development goal 5. URL: <https://www.unwomen.org/en/news-stories/in-focus/2022/08/in-focus-sustainable-development-goal-5>.
- Women, U., n.d. Concepts and definitions. URL: <https://www.un.org/womenwatch/osagi/conceptsanddefinitions.htm>.
- Xiao, Y., Watson, M., 2019. Guidance on conducting a systematic literature review. *Journal of Planning Education and Research* 39, 93–112. URL: <https://doi.org/10.1177/0739456X17723971>, doi:10.1177/0739456X17723971.
- Zacharia, Z.C., Hovardas, T., Xenofontos, N., Pavlou, I., Irakleous, M., 2020. Education and employment of women in science, technology and the digital economy, including AI and its influence on gender equality. Technical Report. European Parliament. URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651042/IPOL_STU\(2020\)651042_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651042/IPOL_STU(2020)651042_EN.pdf).