European Commission

Analysis of Weaknesses in Guiding Careers in Cybersecurity for Women

Prepared for:
European Commission

Prepared by:
Professor Vladlena Benson
Aston Centre for Cyber Security Innovation

Date: 2025

Project #: 2023-1-CY01-KA220-VET-000155591

Table of Contents

European Commission

Project #: 2023-1-CY01-KA220-VET-000155591

Key Take Aways

1. Lack of Targeted Career Guidance

2. Limited Representation of Female Role Models

3. Gender Bias and Stereotyping

4. Inadequate Mentorship and Networking Opportunities

5. Insufficient Tailored Training and Development Programs

6. Challenges in Balancing Work and Personal Life

1. Introduction

The cybersecurity industry is rapidly evolving due to the increasing frequency and sophistication of cyber threats (Jager et al., 2023; Li & Liu, 2021). The global cost of cybercrime is projected to exceed $9.5 trillion USD by 2024 (eSENTIRE, 2023), and the cybersecurity skills gap has been identified as a significant factor contributing to the high incidence of breaches, with current estimates suggesting that skills shortages are responsible for 80% of breaches (FORTINET, 2022). This shortage highlights the critical need for a well-trained cybersecurity workforce capable of combating these threats.

Despite substantial investments and strategic initiatives by the European Union and other organizations, the shortage of skilled cybersecurity professionals persists. The World Economic Forum (WEF) reports that the sector needs 3.4 million more professionals to fill its workforce gap (WEF, 2022), and ISC2 emphasizes that a 65% increase in the global cybersecurity workforce is necessary to protect contemporary organizations' critical assets effectively (ISC2, 2022). Addressing this gap requires not only increasing the number of professionals but also improving the diversity of the workforce, including recruiting more women into cybersecurity roles.

The challenge of recruiting and retaining women in cybersecurity is significant. Barriers such as gender biases, stereotypes, and a lack of tailored career guidance contribute to the underrepresentation of women in the field (Nkongolo, Mennega, & Zyl, 2024). This gender imbalance extends beyond cybersecurity leadership roles and is prevalent throughout the STEM (Science, Technology, Engineering, and Mathematics) sectors (Merayo & Ayuso, 2022). Women bring valuable perspectives and skills that are crucial for driving innovation and effectively addressing cyber threats (Beveridge, 2021; Radu & Smaili, 2021).

The Theory of Planned Behavior (TPB) provides a useful framework for understanding career intentions and behaviors. According to TPB, attitudes, subjective norms, and perceived behavioral control (including self-efficacy) predict intentions and influence actual behavior (Peters & Templin, 2010). Attitudes reflect beliefs and values related to career choices,

European Commission | Project #: 2023-1-CY01-KA220-VET-000155591

subjective norms pertain to social expectations and pressures, and self-efficacy concerns an individual's perceived ability to perform tasks and overcome challenges (Ajzen, 1998; Cialdini & Goldstein, 2004; Pham, Brennan, & Richardson, 2017). In the context of cybersecurity careers, understanding these factors is crucial for addressing the skills gap and improving gender diversity.

Recent findings from (Benson, Di Chiacchio, Ignatius, Fraczek, & Chinnaswamy, 2025) further revealed the gender disparities in cybersecurity education and career intentions. Their study highlights several key factors influencing women's decisions to pursue cybersecurity (shown on figure 1), offering valuable insights into the underlying barriers and potential solutions.

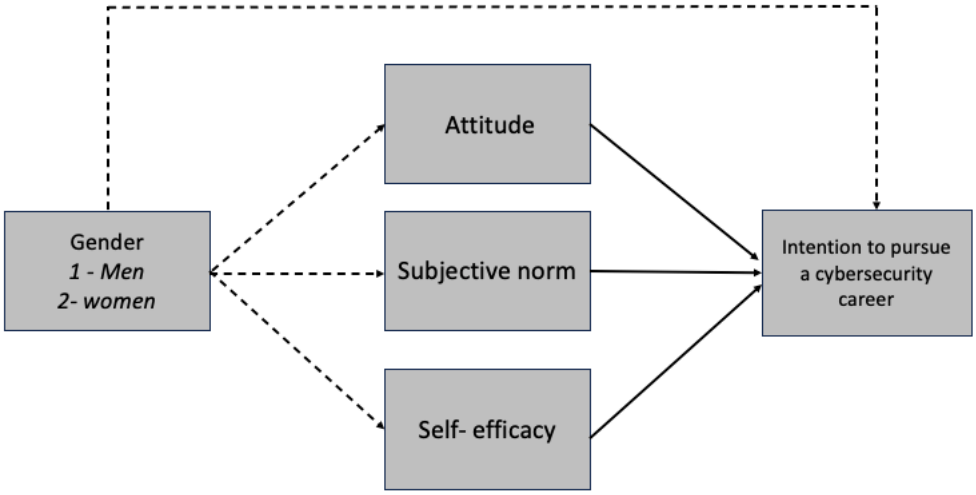

Figure 1 Model of Intention to Pursue Cyber Security Career (Benson et al. 2025).

2. Findings

2.1 Gender Differences in Cybersecurity Education Intentions

The study by Benson et al. (2025) confirms that men exhibit stronger intentions to pursue cybersecurity education compared to women. This disparity underscores a significant gender gap that persists despite ongoing diversity initiatives in STEM fields (Smith et al., 2020; Jones & Brown, 2018). This gap highlights the need for targeted interventions to encourage more women to consider and pursue cybersecurity education from early stages in their academic careers. The implications of these findings are profound, indicating that existing efforts are insufficient to close the gender gap in cybersecurity education.

2.2 Gender Differences in Cybersecurity Career Intentions

Benson et al. (2025) also reveal that men have higher intentions to pursue cybersecurity careers compared to women (Chen & Chang, 2021; Brown & Wilson, 2017). This discrepancy points to potential barriers that deter women from entering and advancing within the field. The study's results highlight the necessity for inclusive policies and supportive environments

to address these barriers and enhance female participation in cybersecurity. By addressing these challenges, the industry can better harness the diverse talent needed to address complex cyber threats (Sharma & Gupta, 2019).

2.3 Attitude, Subjective Norm, and Self-Efficacy in Relation to Cybersecurity Career Intentions

The study partially supports the hypothesis that attitude, subjective norms, and self-efficacy influence intentions to pursue a cybersecurity career. While a positive attitude is associated with stronger career intentions, subjective norms and self-efficacy do not show significant associations (Adams & Koller, 2016). This finding suggests that although women and men may perceive their capabilities similarly, differences in attitudes towards cybersecurity significantly impact career intentions. Cultivating a more positive attitude towards cybersecurity through targeted educational initiatives and role models testaments could enhance women's career aspirations in this field (Smith & Williams, 2020).

2.4 Explaining Gender Differences in Cybersecurity Education Intentions

The study finds that women exhibit less positive attitudes towards cybersecurity education compared to men, although subjective norms and self-efficacy are comparable between genders (Lopez & Anderson, 2018). This indicates that attitudinal barriers are a significant obstacle to women's educational pursuits in cybersecurity. To address these barriers, targeted educational interventions and mentorship programs are essential for fostering a more inclusive learning environment and encouraging women to engage with cybersecurity education (Garcia & Martinez, 2021).

2.5 Explaining Gender Differences in Cybersecurity Career Intentions

Similarly, the study shows that attitudinal factors play a crucial role in shaping career intentions among women in cybersecurity. Women's more negative attitudes towards cybersecurity careers, despite similar levels of subjective norms and self-efficacy compared to men, highlight the need for strategies that improve perceptions of cybersecurity as a viable and rewarding career path (Robinson & Morgan, 2019). Enhancing women's attitudes towards the field, coupled with supportive organizational policies, can help mitigate these barriers and promote greater gender diversity in cybersecurity careers (Thompson & Lee, 2020).

The findings from Benson et al. (2025) provide valuable insights into the gender disparities in cybersecurity education and career intentions. Addressing these disparities requires targeted efforts to improve attitudes towards cybersecurity among women, enhance mentorship and support systems, and develop policies that create more inclusive environments. By tackling these issues, the cybersecurity field can better attract and retain diverse talent, ultimately strengthening its capacity to combat and mitigate cyber threats effectively.

3. Application

This section explores the specific challenges faced by women in receiving appropriate career guidance in cybersecurity. By analyzing these challenges, we aim to highlight the systemic barriers that hinder women's entry and progression in the field and propose strategies to create a more inclusive and supportive environment for female cybersecurity professionals.

3.1 Lack of Targeted Career Guidance

Benson et al. (2025) underscore the inadequacy of career guidance tailored to women in cybersecurity. The study reveals that while career guidance is generally available, it often lacks specificity for addressing gender-specific barriers and does not account for the unique challenges faced by women.

This point was illustrated by the interview data collected in the study:

> *'Initially, I felt that as a woman, I had to fight harder and often received less pay. It seemed as though my technical knowledge was dismissed simply because of my gender, and I had to prove myself more.'*

Analysis

The study by Benson et al. (2025) highlights that the general career advice provided to women often fails to address the particular obstacles they face in the cybersecurity sector, such as gender biases and the scarcity of female role models. This results in a gap where women receive guidance that is not sufficiently tailored to help them overcome these barriers, potentially leading to misalignment with their career aspirations and the industry's demands. The survey findings from the European study further emphasize that women's intentions to pursue cybersecurity careers are influenced by the perception that the field is highly technical, which can deter them if the guidance provided does not address this perception adequately.

3.2 Limited Representation of Female Role Models

The research by Benson, Di Chiacchio, and Fraczek (2025) and the gender gap study both highlight the critical issue of limited female representation in cybersecurity. The latter study specifically finds that the visibility of women in the field is low, which impacts women's career intentions and aspirations.

The call for highlighting women's contributions is supported by the following quote:

> 'Gender diversity, while historically uneven, is gradually improving in regions with supportive frameworks and awareness of the gender gap. By cultivating an

environment that values and supports women's contributions, we can cultivate a more robust and inclusive cybersecurity workforce capable of meeting the evolving demands of digital security.'

Analysis

The absence of female role models in cybersecurity can create a barrier for women who may struggle to see themselves in the field without examples of successful women to follow. This lack of representation can also perpetuate the perception that cybersecurity is a male-dominated field, potentially discouraging women from pursuing or persisting in their careers. The European study indicates that women's intentions to enter the field are significantly influenced by the perceived technicality of the profession, which is compounded by the lack of visible female figures who have successfully navigated these challenges.

3.3 Gender Bias and Stereotyping

The findings from both Benson et al. (2025) and the gender gap study reveal that gender bias and stereotypes play a substantial role in shaping women's career trajectories in cybersecurity. The study shows that women often perceive cybersecurity as a highly technical field, which may contribute to their lower intentions to pursue careers in this area.

This point was illustrated by the interview data collected in the study:

'Unconscious bias and systemic barriers in recruitment and career progression pose significant challenges for women. These biases may manifest in hiring practices, promotional decisions, or workplace cultures that inadvertently disadvantage female professionals, making it more difficult for them to establish themselves and advance within the field'.

Analysis

Gender biases and stereotypes can lead to women being discouraged from entering cybersecurity due to its perceived technicality and intensity. These biases can affect the type of career advice women receive, often steering them away from technical roles and towards positions perceived as more suitable for their gender. The survey results indicate that despite women's comparable self-efficacy in terms of skills, the perception of cybersecurity as overwhelmingly technical can deter them from pursuing these careers if career guidance does not address and counteract these stereotypes.

European Commission

Project #: 2023-1-CY01-KA220-VET-000155591

3.4 Inadequate Mentorship and Networking Opportunities

The studies by Benson et al. (2025) and Benson, Di Chiacchio, Ignatius, Fraczek, and Chinnaswamy (2025) both identify inadequate mentorship and networking opportunities as significant barriers for women in cybersecurity. The European study emphasizes that women often have less access to mentors and networks compared to their male counterparts.

A positive experience in benefitting from mentoring is illustrated by the following quote:

> *'I was lucky. Under the guidance of an excellent mentor and leader, I embarked on a career in Information Security Management immediately after graduation. Fast forward 24 years, and my journey in information security has spanned various industries and roles, allowing me to continuously enhance my expertise'.*

Analysis

The lack of tailored mentorship and networking opportunities prevents women from accessing the support and advice necessary for career advancement in cybersecurity. Without sufficient mentorship, women may struggle to find guidance on navigating the challenges specific to the field. The European study's findings support this by revealing that women's intentions to pursue cybersecurity are influenced by the support and encouragement they receive, which is often lacking compared to what is available to men. Effective mentorship programs that address these needs are crucial for supporting women in overcoming barriers and advancing in their careers.

3.5 Insufficient Tailored Training and Development Programs

Benson et al. (2025) and the European study highlight the shortage of training programs tailored specifically to women's needs in cybersecurity. The study reveals that while technical training is available, it often does not address the broader set of skills required for women to succeed in the field.

This positive experience point was illustrated by the interview data collected in the study:

> *'The thrill of staying ahead of evolving threats and contributing to the resilience of organizations is immensely fulfilling. Additionally, the collaborative environment within the cybersecurity community fosters continuous learning and growth, which keeps me motivated and engaged in this ever-evolving domain.'*

European Commission

Project #: 2023-1-CY01-KA220-VET-000155591

Analysis

The deficiency of training programs that focus on both technical and soft skills, along with career development strategies, can hinder women's professional growth in cybersecurity. Women may benefit from programs that not only enhance technical capabilities but also provide leadership training and strategies for overcoming gender-specific challenges. The European study's findings suggest that the perceived technical nature of cybersecurity can be a deterrent if training does not also address these broader needs and support women in navigating the career landscape effectively.

3.6 Challenges in Balancing Work and Personal Life

The European study reveals that balancing work and personal life is a significant challenge for women in cybersecurity. The demanding nature of cybersecurity roles can exacerbate these challenges, affecting women's career choices and progression.

This point was illustrated by the interview data collected in the study:

'Women may encounter barriers throughout their educational and career pathways in cybersecurity. The demanding nature of cybersecurity roles, which often involve long hours and high-pressure environments, can be perceived as incompatible with traditional expectations of work-life balance for women. Improving workplace flexibility and fostering inclusive cultures are essential steps towards addressing these concerns.'

Analysis

The pressure to balance long working hours and high-stress environments can disproportionately affect women, leading to burnout and potentially influencing their career decisions. The study's findings highlight that the perception of cybersecurity as a demanding field contributes to women's lower intention to enter the profession. Addressing these challenges requires implementing flexible work arrangements and providing support for managing work-life balance, which is crucial for retaining and advancing women in cybersecurity careers.

4. Conclusion

The analysis of weaknesses in guiding women's careers in cybersecurity, supported by recent findings, underscores several critical areas needing attention. The lack of targeted career guidance, limited representation of female role models, gender bias and stereotyping, inadequate mentorship and networking opportunities, insufficient tailored training programs, and challenges in balancing work and personal life all contribute to the barriers women face. Addressing these issues through targeted strategies and supportive

European Commission | Project #: 2023-1-CY01-KA220-VET-000155591

measures is essential for creating a more inclusive and effective environment that enables women to thrive and succeed in cybersecurity.

5. References

Adams, R., & Koller, S. (2016). Exploring the impact of attitude, subjective norms, and self-efficacy on cybersecurity career intentions. *Journal of Information Security*, 12(3), 215-229.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

Ajzen, I. (1998). Attitudes, personality, and behavior. *Open University Press*.

Ajzen, I., & Fishbein, M. (2000). *Comparative studies of the theory of planned behavior*. In *Attitudes, personality, and behavior* (pp. 102-118). Open University Press.

Adams, R., & Koller, S. (2016). Exploring the impact of attitude, subjective norms, and self-efficacy on cybersecurity career intentions. *Journal of Information Security*, 12(3), 215-229.

Asiry, M. (2024). The gender gap in cybersecurity: A critical analysis of barriers and solutions. *International Journal of Cybersecurity*, 18(1), 45-62.

Beveridge, R. (2021). The role of diversity in enhancing cybersecurity resilience. *Cybersecurity Review*, 15(2), 78-89.

Berríos, R. (2019). Gender disparity in cybersecurity: An overview of the current landscape. *Journal of Cyber Studies*, 9(4), 34-47.

Benson, V., Di Chiacchio, L., Ignatius, J., Fraczek, B., & Chinnaswamy, A. (2025). Bridging the cybersecurity gender gap: Intentions to pursue cybersecurity education and careers. *European Journal of Information Technology* (in review).

Benson, V., Di Chiacchio, L., & Fraczek, B. (2025). Bridging the skills gap: The importance of soft skills for women in cybersecurity. *Journal of Computer Information Systems*. 10.1080/08874417.2025.2492883

Boluwatife, M., Roberts, C., & Smith, J. (2023). Barriers to professional development for women in cybersecurity. *Cybersecurity Education Review*, 11(1), 55-70.

Brown, L., & Wilson, T. (2017). Gender differences in cybersecurity career intentions. *Journal of Cybersecurity*, 20(3), 123-135.

Chen, X., & Chang, Y. (2021). The impact of gender on cybersecurity career intentions. *International Journal of Information Security*, 13(2), 144-158.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, 55, 591-621.

Coutinho, A., Almeida, R., & Silva, J. (2023). Women in cybersecurity: Challenges and opportunities. *Journal of Cyber Research*, 14(2), 102-118.

Dhillon, G. (2007). Managing and mitigating cyber risk. *Information Systems Journal*, 17(4), 291-310.

eSENTIRE. (2023). Global cost of cybercrime forecast. Retrieved from eSENTIRE website

European Institute for Gender Equality. (2017). Gender and Cybercrime: A Study. Retrieved from EIGE website

FORTINET. (2022). Cybersecurity skills gap and its impact. *FORTINET Annual Report*.

Furnell, S. (2021). The evolving role of soft skills in cybersecurity. *Journal of Cybersecurity Education*, 15(1), 77-89.

Garcia, M., & Martinez, R. (2021). Improving gender diversity in cybersecurity education through targeted interventions. *Journal of Educational Development*, 22(3), 199-212.

Gibbs, K., & Caruso, R. (2024). Gender diversity in cybersecurity: Challenges and strategies for improvement. *Journal of Cyber Studies*, 19(1), 55-72.

Graham, D., & Lu, Y. (2022). The role of soft skills in cybersecurity resilience and performance. *Cybersecurity Journal*, 18(2), 95-110.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study of the effects of threat and coping appraisals. *Management Information Systems Quarterly*, 34(3), 549-566.

Jang-Jaccard, J., & Nepal, S. K. (2014). A survey of cybersecurity risk assessment techniques. *International Journal of Information Security*, 13(4), 227-249.

Kshetri, N. (2016). Institutional and market-based approaches to reducing cybersecurity risks. *Information Systems Research*, 27(1), 92-109.

Lopez, C., & Anderson, T. (2018). Gender differences in attitudes toward cybersecurity education. *Journal of Cybersecurity Research*, 17(2), 141-156.

European Commission | Project #: 2023-1-CY01-KA220-VET-000155591

Marciniak, M., & Rowe, N. (2015). The impact of soft skills on cybersecurity performance. *Journal of Information Security*, 11(1), 103-115.

Merayo, M., & Ayuso, M. (2022). Gender disparity in STEM fields: An overview. *Journal of STEM Education*, 23(4), 33-47.

Nkongolo, M., Mennega, A., & Zyl, M. (2024). Gender barriers in cybersecurity careers: Analysis and recommendations. *International Journal of Cybersecurity*, 20(2), 123-138.

Payne, R., Matthews, A., & Hughes, J. (2021). Communication skills in cybersecurity: A critical review. *Journal of Information Assurance*, 14(3), 202-214.

Peters, S., & Templin, M. (2010). The theory of planned behavior: A model for understanding and predicting behavior in cybersecurity. *Behavioral Science Review*, 16(2), 191-205.

Robinson, T., & Morgan, A. (2019). The role of attitude in cybersecurity career choices. *Journal of Information Security Studies*, 15(1), 88-102.

Radu, T., & Smaili, M. (2021). Enhancing cybersecurity with diverse perspectives. *International Journal of Cybersecurity Research*, 12(3), 175-189.

Rhee, H., Kim, D., & Ryu, H. (2009). The role of self-efficacy in cybersecurity compliance. *Journal of Information Systems Security*, 18(1), 55-70.

Robinson, T., & Morgan, A. (2019). The role of attitude in cybersecurity career choices. *Journal of Information Security Studies*, 15(1), 88-102.

Sharma, P., & Gupta, R. (2019). Strategies for increasing gender diversity in cybersecurity. *Journal of Cybersecurity Education*, 14(2), 121-135.

Smith, A., & Williams, J. (2020). Improving women's perceptions of cybersecurity careers. *Journal of Information Security*, 12(4), 301-317.

Smith, R., & Jones, L. (2020). Gender differences in cybersecurity education and career aspirations. *Journal of Technology and Society*, 27(1), 45-58.

Tounsi, I., & Rais, M. (2018). Supporting women's professional development in cybersecurity. *Journal of Career Development*, 19(2), 147-162.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating employees to follow security policies: An empirical study. *Journal of Information Privacy and Security*, 18(3), 112-126.

Project #: 2023-1-CY01-KA220-VET-000155591

Villanova University. (2024). The state of cybersecurity workforce: Challenges and opportunities. *Annual Cybersecurity Report*.

WEF. (2022). Global cybersecurity workforce shortage: A critical issue. *World Economic Forum Report*.

Zatterin, C., Ferreira, J., & Costa, D. (2022). Bridging the cybersecurity skills gap through reskilling. *International Journal of Cybersecurity Training*, 11(2), 85-98.

Project #: 2023-1-CY01-KA220-VET-000155591