

GENDER-BASED CYBERSECURITY SKILLS GAP

Mariam Khobelia, Salome Petriashvili

Revised by: Elena Tsatsua

Abstract

The gender-based cybersecurity skills gap represents a significant challenge in the cybersecurity industry, with women comprising only about 24% of the workforce despite recent improvements. This disparity not only reflects gender inequality but also means missing out on the valuable perspectives that women bring to solving complex cybersecurity problems. This study looks at the current state of gender diversity in cybersecurity and the obstacles women face, such as stereotypes, lack of mentors, pay gaps, and fewer career opportunities. Using surveys and interviews, the research shows that having more women in cybersecurity can improve team performance, creativity, and overall security. The paper also reviews current efforts to close this gap, including partnerships, mentorship programs, and educational initiatives. The findings highlight the need for strong action from industry leaders to build a more inclusive and diverse cybersecurity workforce, which will ultimately strengthen global cybersecurity.

Introduction

The field of cybersecurity plays an increasingly vital role in safeguarding our digital infrastructure and personal information. As cyber threats continue to evolve in complexity and frequency, the demand for skilled cybersecurity professionals is at an all-time high. However, despite efforts to diversify the workforce, women remain significantly underrepresented, comprising only about 24% of cybersecurity professionals globally according to recent studies (ISC)² Cybersecurity Workforce Study, 2020). This gender disparity not only highlights ongoing gender inequalities but also underscores missed opportunities to leverage diverse perspectives in addressing cybersecurity challenges effectively.

In recent years, the cybersecurity industry has recognized the importance of diversity, not only as a matter of equity but also as a strategic advantage. Research indicates that diverse teams, including those with gender diversity, tend to perform better in terms of innovation, problem-solving, and overall team dynamics (McKinsey & Company, 2018). However, women continue to face numerous obstacles in entering and advancing within the cybersecurity field.

Obstacles such as stereotypes, lack of mentorship, pay gaps, and limited career advancement opportunities persist, hindering the full participation of women in cybersecurity roles. Stereotypes that associate technical fields with masculinity discourage young women from pursuing careers in cybersecurity, perpetuating a cycle of underrepresentation. Furthermore, the absence of visible role models and mentors deprives aspiring women of crucial guidance and support needed to navigate and excel in this challenging domain.

Addressing these challenges requires proactive measures from industry leaders, educational institutions, and policymakers. Efforts such as mentorship programs, educational initiatives, and partnerships between academia and industry are crucial steps towards fostering a more inclusive and diverse cybersecurity workforce. These initiatives not only aim to increase the number of women in cybersecurity but also to create an environment where all individuals, regardless of gender, can thrive and contribute effectively.

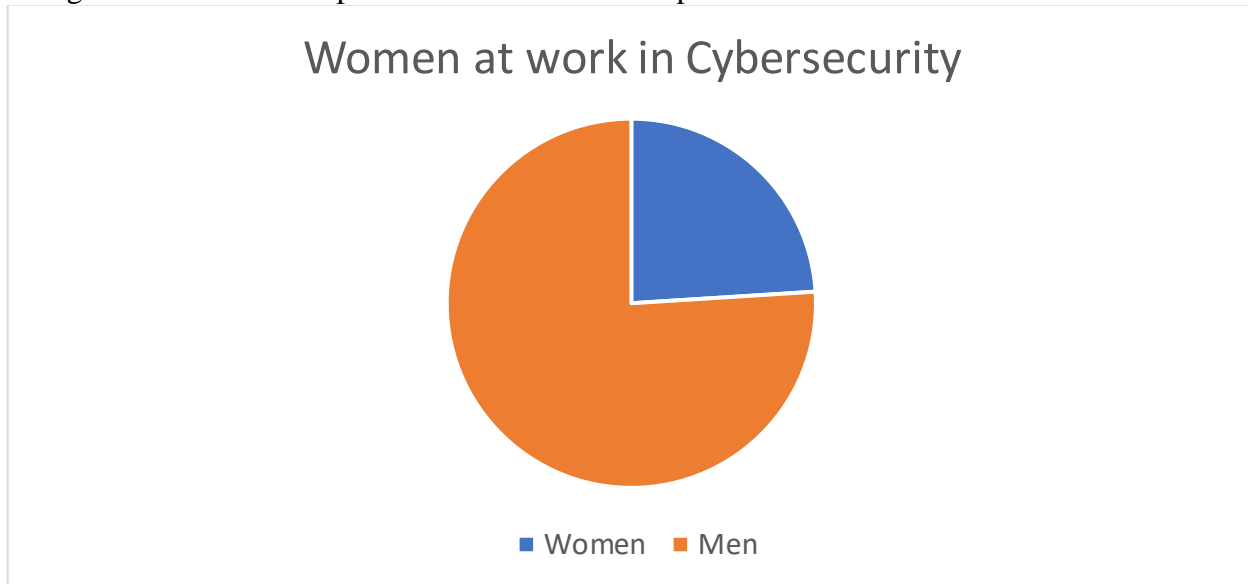
This study seeks to explore the current state of gender diversity in cybersecurity, identify the barriers that women face, and examine the impact of gender diversity on team performance, creativity, and cybersecurity outcomes. By examining survey data and conducting interviews with industry

First Student Conference: “Gender Dimension of CyberSecurity”

professionals, this research aims to provide insights into effective strategies for closing the gender-based cybersecurity skills gap and building a resilient and inclusive cybersecurity workforce for the future.

Current State of Gender Diversity in Cybersecurity

According to the (ISC)² Cybersecurity Workforce Study (2020), women make up only about 24% of the global cybersecurity workforce. This figure underscores a persistent gender disparity in a field critical to global digital security. While there have been incremental improvements in recent years, the rate of change remains slow compared to other STEM disciplines.

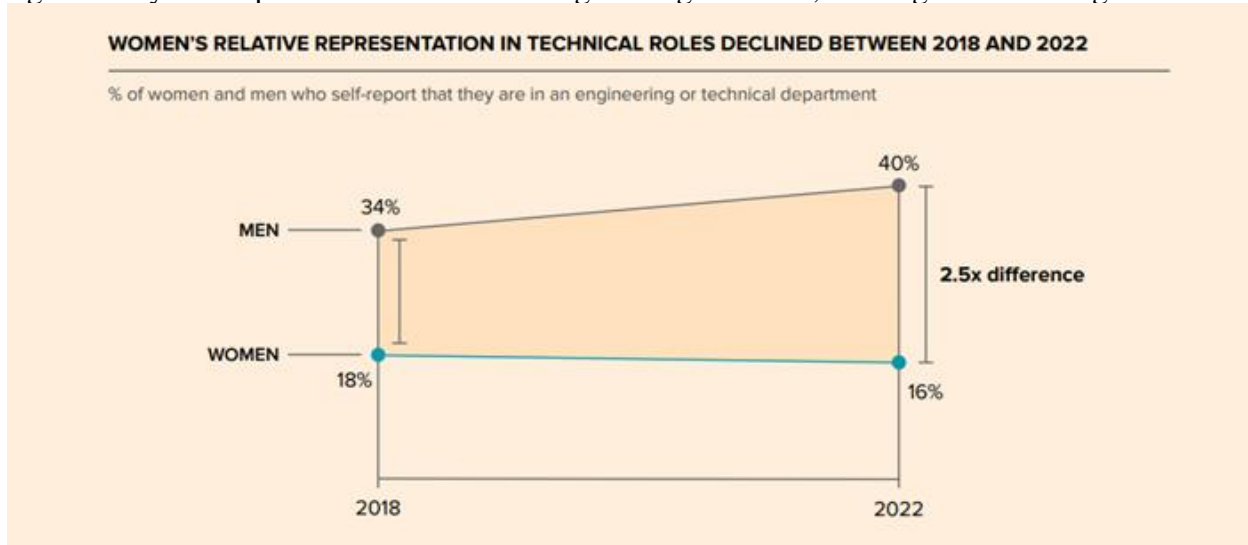


(ISC)² Cybersecurity Workforce Study

Gender Equality in Digital Sphere

32% of women in technical and engineering roles are often “the only woman in the room” at work, according to the McKinsey report “Women in the Workplace 2022.”

This can partially explain why women in tech face a higher level of gender bias. Women are also significantly less represented than men in engineering and tech, with figures declining since 2018.



McKinsey study “Women in the Workplace

First Student Conference: “Gender Dimension of CyberSecurity”

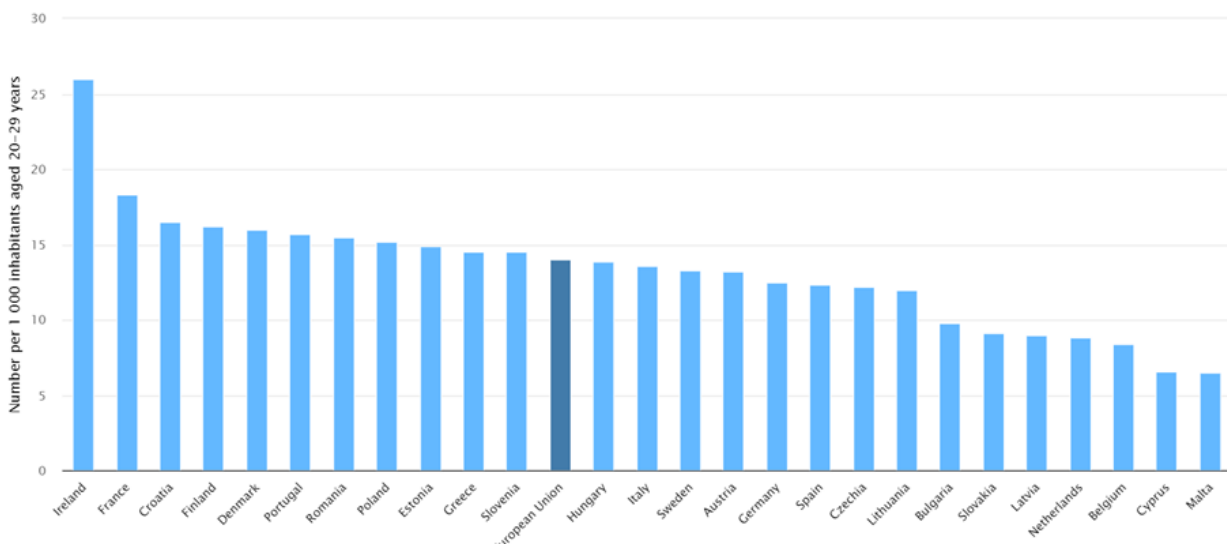
The Situation in Europe

In Europe, just 14% of STEM (Science, Technology, Engineering and Mathematics) graduates are women, while 28% are men. This gap reflects the significant gender inequality in this area. Countries like Finland, Sweden, Denmark, Estonia, and the Netherlands have the best scores in terms of female participation in digital sectors, with percentages ranging from 64.6% to 76.9%. These countries also get good results in the DESI (Digital Economy and Society Index).

Yet Romania, Bulgaria, Poland, Hungary, and Italy have lower percentages in terms of female participation, with scores ranging from 36.2% to 43.8%.

For the “STEM graduates” indicator, the best performing countries are Ireland, France, Croatia, Finland, and Denmark, with a high number of female graduates in science, technology, engineering or mathematics per 1000 individuals aged 20-29.

3.1 STEM graduates, Females, 16 to 74 years old
Year: 2020



source:

Eurostat

Why The Field Needs More Women

them, which can help organizations understand and address issues that may be overlooked otherwise. For example, severe online harassment and the practice known as doxxing (the intentional, nonconsensual exposure of an individual’s private information online) disproportionately affect marginalized groups including women, according to a 2021 Pew Research Center poll.

Moreover, a gender-diverse team considers a broader range of perspectives, experiences, and problem-solving methods than a heterogenous team. As cyber attacks become more varied and complex, information technology (IT) teams need to harness all the problem-solving tools that they can find.

Effective communication can bridge the gap between technical solutions and the people they protect. Ensuring diverse perspectives are represented can improve collaboration, innovation, and communication within cybersecurity teams and across companies.

As more women work in cybersecurity, organizations are likely to have a larger pool of workers to draw from in the future, because representation matters.

Motivating more women to immerse themselves in the world of cybersecurity paves the way for the mentorship of other women and sparks inspiration for the coming generations. Research reported in Forbes indicates that, when young girls hear about STEM careers from women role models, it positively influences their ambitions in these fields

First Student Conference: “Gender Dimension of CyberSecurity”

Factors That Contribute to the Gender Gap in Cybersecurity

Multiple specialists agree that stereotypes and bias can have a negative influence on aspirations, identity, interests, mindsets, motivation, self-esteem, and personal effectiveness in STEM.

The World Bank’s report underlines the existence of sexist bias in many environments, particularly in education. Data - primarily from Europe and the USA and based on limited samples - confirms these biases. From the start of school (or even before), stereotypes often exist. For example, one study showed that 70% of adults surveyed in 34 countries associate STEM subjects with men.

Educational materials used to teach children can also reflect these stereotypes. According to the same report, several countries such as Bangladesh, China, India, Indonesia, Malaysia, Pakistan, Romania, and the USA have school curricula that reproduce these stereotypes.

Women struggle to feel valid
“Women struggle to feel valid in a profession whose image does not look like them. They will say: “I do IT” more often than: “I’m an IT engineer.” Even though the very first programmer was a woman.” (Isabelle Collet, Monde diplomatique). The image of hackers, largely spread by the media, also reinforces the idea that IT engineers are primarily men passionate about machines.

Solutions to Bridge the Gap

To address these challenges, several solutions can be implemented. Promoting STEM education for young girls is a foundational step. Encouraging interest in technology from an early age helps build a pipeline of future female cybersecurity professionals.

Mentorship and sponsorship programs are vital. Organizations should actively create opportunities for women to connect with mentors who can guide their career development. Inclusive workplace policies, such as equitable pay and anti-discrimination measures, are essential to create a supportive environment. Flexible work arrangements can help women balance professional and personal responsibilities. Highlighting successful women in cybersecurity through media and industry events can provide inspiration and role models for aspiring professionals.

Organizations Supporting Women in Cybersecurity

In recent years, numerous organizations and initiatives have emerged to support and empower women in cybersecurity, aiming to address the gender gap and promote inclusivity within the industry. These programs play a crucial role in providing resources, mentorship, and opportunities for women to thrive in a traditionally male-dominated field. This section explores key organizations dedicated to advancing gender diversity in cybersecurity across different regions.

European Centre for Women and Technology (ECWT)

The European Centre for Women and Technology (ECWT) is a leading advocate for gender equality in STEM fields throughout Europe, with a specific focus on cybersecurity.

Women Techmakers in Georgia

Women Techmakers is a global program from Google that supports and celebrates women in technology, including cybersecurity, with local chapters worldwide, including Georgia.

Case Studies and Real-World Examples

Several organizations have successfully addressed the gender gap. For example, IBM's Women in Security Excelling (WISE) initiative focuses on mentorship, leadership training, and creating opportunities for women in cybersecurity. Similarly, Symantec's Women in Cybersecurity program offers networking and development opportunities specifically tailored for women.

First Student Conference: “Gender Dimension of CyberSecurity”

Stories of women who have overcome challenges in cybersecurity can also provide valuable insights. For instance, Parisa Tabriz, known as Google's "Security Princess," has become a prominent figure in the industry, inspiring many with her achievements and advocacy for diversity.

Conclusion

Closing the gender gap in cybersecurity is critically important for several reasons that go beyond mere equity. First and foremost, diversity in cybersecurity teams brings a variety of perspectives and approaches to problem-solving. Women, who are currently underrepresented in the field, offer unique insights that can lead to more innovative solutions and more effective strategies for protecting digital assets and infrastructure.

Moreover, increasing the participation of women in cybersecurity helps to alleviate the severe talent shortage that the industry is currently facing. By tapping into a broader talent pool, organizations can fill critical roles more effectively and strengthen their overall cybersecurity posture.

Additionally, promoting gender diversity fosters a more inclusive workplace culture. This not only enhances employee morale and satisfaction but also improves retention rates within the industry. When women feel valued and respected in their roles, they are more likely to stay and contribute to the long-term success of their organizations.

In conclusion, closing the gender gap in cybersecurity is not just a matter of social justice; it is a strategic imperative for the industry's growth, innovation, and effectiveness in combating cyber threats. By actively working towards greater gender diversity and inclusion, stakeholders can create stronger, more resilient cybersecurity teams that are better equipped to face the challenges of tomorrow's digital landscape. This requires concerted efforts from educational institutions, industry leaders, policymakers, and individual professionals to create a future where cybersecurity is truly a field that welcomes and benefits from the talents of all individuals, regardless of gender.

References

1. <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Women-in-Cybersecurity-Report.pdf?rev=d9c1e6269f8d43b19ee8fae5972a1bf5#:~:text=Nearly%20half%20of%20women%20cybersecurity%20professionals%20surveyed%20are,about%20one%20quarter%20%2824%25%29%20of%20the%20overall%20workforce.>
2. <https://www.threatkey.com/resource/the-gender-gap-in-cybersecurity-challenges-and-solutions>
3. <https://online.utulsa.edu/blog/gender-diversity-in-cybersecurity/#:~:text=Gender%20Diversity%20in%20Cybersecurity%20Provides%20Broader%20Perspectives%20Gender,and%20address%20issues%20that%20may%20be%20overlooked%20otherwise.>
4. <https://gdgtbilisi.blogspot.com/>
5. <https://www.orange cyberdefense.com/uk/insights/blog/career/for-a-safer-digital-society-breaking-down-gender-barriers-in-cybersecurity#c86721>
6. McKinsey study “Women in the Workplace
7. Eurostat