Cybersecurity and Innovation Technology Journal, Vol.3, No.1, 2025, pp. 1-8
e-ISSN 3025-6682. DOI. 10.52889/citj.v3i1.622

Digital Divide in Cybersecurity

Submitted 13 April 2025, Revised Date 26 April 2025, Accepted 27 April 2025

William J. Triplett[1,2*]

[1]Health Information Technology Program, Department of Information Systems,
University of Maryland, Baltimore County, Baltimore, United States

[2]Cybersecurity Leadership Program, Department of Healthcare Technology,
Capitol Technology University, Laurel, United States
Corresponding Email: *wjtriplett@captechu.edu

Abstract

The digital gap actively determines how people obtain varying degrees of access to technological resources, educational opportunities, and job opportunities, specifically within cybersecurity. Research explores digital divide patterns in cybersecurity populations by analyzing unequal opportunities related to cybersecurity education, job opportunities, and security protection levels. This study combines demographic analytics and interview data to reveal how socioeconomic standing, racial background, gender identities, and regional locations simultaneously shape cybersecurity accessibility and workforce take-up. The data reveals systemic obstacles between low-income citizens and minority groups while closing access to awareness regarding entry into cybersecurity roles. The study ends by suggesting policy and educational outreach reforms that might eliminate digital inequalities.

Keywords: Cybersecurity, Digital Divide, Demographics, Underrepresentation, Digital Equity

INTRODUCTION

The digital economy's participation and benefits remain out of reach for many people, although digital tools and networks have become fundamental for modern life (Williams, 2021). Education, employment, health, and security face the direct consequences of this digital gap. In cybersecurity settings, the digital divide determines which populations face maximum threats and who becomes a member of protective defense teams. Existing research explores the digital divide phenomenon and cybersecurity work diversity but lacks detailed studies on how the digital divide shapes cybersecurity labor statistics. This paper explores that gap.

The cybersecurity sector rapidly demands more skilled workers because of growing market needs. The pipeline functions with restricted demographics that comprise most of its workforce. Few women and minorities, together with low-income groups and people living in rural areas, make up minority groups in cybersecurity (Wongkrachang, 2023). For developing effective cybersecurity readiness, the frameworks must contain components that represent the everyday experiences of marginalized communities. The nation requires immediate action to resolve this problem. Modern society depends on digital resources to function, but ongoing digital inequities create expanding differences in cybersecurity competence and active involvement between digital groups. Extant research explores the digital divide in general terms. It analyzes cybersecurity workforce diversity separately from one another, although no study exists regarding how the digital divide affects explicitly cybersecurity demographic profiles (Huang, 2024). The research analyzes the dual impact of exclusion on digital security by studying affected populations, exposure risks, and workforce shortages.

Internet connectivity alone does not explain the digital divide because of inseparable factors between education systems, employment structures, and sociocultural dynamics. A complete understanding of the effects of cybersecurity necessitates a research model that analyzes institutional, geographic, and systemic disparities (Calderaro & Craig, 2020). This research fills this knowledge gap by exploring how social group differences maintain inadequate cybersecurity knowledge accessibility, education, and limited professional involvement. Developing an effective cybersecurity readiness framework requires inclusionary systems that address real-life situations marginalized communities face.

The digital divide expanded from basic internet access problems to multifaceted barriers, including digital knowledge gaps, cultural differences, and organizational discrimination. Because of the growing digital threats, cybersecurity problems are receiving more attention at the intersection of this societal gap. Studies indicate that academics notice disparities in the mid-career range when accessing cybersecurity support within the lower to middle levels of the organizational hierarchy, particularly regarding gender. Wongkrachang (2023) draws attention to the lack of active participation by minority groups in cybersecurity and emphasizes the need for fundamental transformation. Chukwurah *et al.* (2024) explore problem-solving methods to increase inclusiveness in protecting computer systems, while AlDaajeh *et al.* (2022) illustrate the importance of equitable educational policies for aiding neglected populations in developing skills in cybersecurity. As such, national policy on cybersecurity should incorporate programs on the equitable provision of education and employment.

The process of representation with culturally relevant pedagogy serves as a vital method to break down barriers. Education reform, policy-led innovation, and localized outreach represent this scholarly group's core recommendations (Shanley, 2021). Research now highlights two major aspects regarding workforce participation while simultaneously exploring the impact of algorithmic bias alongside surveillance methods on marginalized groups. The security enhancements built to fight cyber attacks often end up watching and suspecting users from minority groups while sustaining the existing biases of the system. The digital civil rights situation highlights the ethical importance of creating equal cybersecurity systems for all groups. Research gaps persist even though studies have explained how artificial intelligence supports digital security projects and sustains the workforce. This research explores the issue through statistical information and narrative data analysis.

METHOD

The research design used quantitative demographic analysis and qualitative interview data collection methods. Both groups of participants were included in the study. Government and industrial reports provided data about cybersecurity workforce demographics through public listings. Twenty interviewees from underrepresented groups, like women, BIPOC, and low-income and rural participants who pursued or practiced cybersecurity, formed the second participant group. Two methods were used to gather research data: (1) data scraping software alongside content analysis programs for workforce data collection and (2) semi-structured interview guides, which examined cybersecurity education access, professional barriers, and career paths. The research collected quantitative information through reports spanning from 2020 to 2024, which were retrieved from the U.S. Department of Labor alongside ISC2 and CompTIA. The researcher conducted Zoom-based virtual interviews lasting 45 to 60 minutes each.

The analysis of numerical data employed statistical descriptions and comparisons between demographics. The analysis used grounded theory methods to code interview transcripts for dominant patterns that described both exclusion and cybersecurity opportunities. The research followed supplementary procedures to verify data reliability as well as validity. A triangulation strategy employed checking results between various data collections from participants and analytic dimensions. A member-checking procedure involved sharing findings summaries with participants for their feedback to increase the quality of qualitative analysis credibility. The researcher protected subject integrity through ethical procedures before getting Institutional Review Board (IRB) approval to start data collection. The cybersecurity research should incorporate methodological inclusivity because it reveals underlying systematic obstacles.

RESULTS AND DISCUSSION

The analyzed research about digital inequality backs previous findings, yet it creates new insights through analyzing structural barriers and emotional restrictions. Students who encounter technology early in their schooling develop growing confidence, which leads them to pursue cybersecurity professions. The lack of funding in schools usually eliminates these pathways (Braveman *et al.,* 2022). Moreover, intersectionality intensifies exclusion. A rural Latina from a low-income background encounters multiple barriers blocking her path, which urban affluent male peers do not need to overcome. Strategies need to be customized with outreach that targets specific areas while providing financial assistance, besides developing multicultural curricula.

National policy should establish cybersecurity equity as a top priority (AlDaajeh & Alrabaee, 2024). McBride *et al.* (2022) advocate for implementing cybersecurity within STEM educational programs at community colleges. Gonzalez (2021) describes how programs based on mentorship and retention should specifically target BIPOC professionals. The proposed solutions demonstrate promise, even though adequate funding is scarce.

Public-private partnerships are another solution. HBCUs and tribal colleges, together with community organizations, can co-create apprenticeship programs and training schemes with the support of corporate businesses. Barile *et al.* (2023) propose dual training structures that unite operational skills development with ethical and supporting frameworks. Evaluations call for changes to hiring standards, which depend on conventional qualifications for employment. Employers should review their employee competency evaluation methods, through which they could include portfolios, peer reviews, and community endorsements during candidate selection. Such inclusivity efforts will result in a more resilient professional cybersecurity workforce representing the diverse national population. Statistical data showed that women comprised only 24% of the cybersecurity workforce, while all other demographic groups remained below this percentage. The workforce data demonstrates that African Americans represent only 9%, while Latinos comprise 8% of the total professionals (Salsberg *et al.,* 2021). Each rural state contained a limited number of cybersecurity professionals compared to its total population count.

Underrepresented groups faced increased disparities in entry-level and mid-career positions because they identified fewer professional growth opportunities. Black and Hispanic cybersecurity professionals and women experienced slower career advancement and reduced professional retention rates (Prewitt, 2024). Cybersecurity hiring shows an urban bias because little money is put into rural tribes or underdeveloped areas for cybersecurity talent training. Both organizational and geographic barriers exist that block underrepresented groups from participating in the workforce.

Qualitative interviews. Reinforced these findings. Key themes included:

1. **Access Barriers:** Participants noted that high-speed internet is often unavailable in rural areas and low-income urban regions, classifying this as a further lack of access.
2. **Education Gaps:** The lack of high school and community college programs offering cybersecurity courses was cited as an educational gap.

3. **Economic Constraints:** Several respondents highlighted economic barriers that stem from the high costs of certification programs like CISSP and Security +.
4. **Representation:** A number of interviewees expressed feeling disenfranchised in the context of study or work because of the lack of representatives from their communities.

The research revealed two main problems concerning institutional trust and systemic bias concerns among the participant group. The analyses of this study articulated their skepticism about standard educational procedures because professional institutions have historically limited their recruitment possibilities. Employers used various evidence to reject qualifications because they did not comprehend alternative education approaches. The collected data indicate that cultural methodology in workforce inclusion must address educational development systems and professional training methods.

Research findings confirm that digital inequality expands cybersecurity flaws while reducing diverse population inclusion. Underfunded schools that do not provide early cybersecurity education block students from pursuing lucrative career positions for many years. The financial as well as cultural obstacles and hurdles in certification and hiring processes further perpetuate unfair treatment.

The qualitative data revealed emotional effects that arise when underrepresentation occurs. The interview participants shared their feelings of anger, a sense of unworthiness and a perspective of segregation. Most cybersecurity educational approaches and workforce preparation methods do not focus on solving these social barriers (Crumpler & Lewis, 2022). Equitable cybersecurity participation requires addressing emotional dimensions through mentorship programs combined with inclusive leadership, while peer support systems for addressing psychosocial barriers should also be implemented. Nobles (2020) explains that cybersecurity plans without cultural intelligence create substantial obstacles to the success of inclusive initiatives.

Multiple demographic characteristics intersect to deliver additional difficulties affecting specific groups. A lower-income Latina living in a rural area will encounter obstacles three times more than those faced by affluent male students living in urban environments. Successfully resolves these multiple barriers needs purposeful planning in program and policy creation that moves away from general assumptions (Head, 2022). The combination of digital literacy training, mentoring, cost-reducing efforts, and outreach based on local areas will most effectively reach these communities. The research supports national cybersecurity development strategies, which must be customized and data-driven.

CONCLUSION

The analysis shows that digital gaps create cybersecurity limitations through educational and professional access denial as well as through unnoticeable psychological barriers. Structural inequity and underrepresentation perpetuate a cycle of digital vulnerability and limited career opportunity.

Bridging this divide will require:

1. Equitable investments in digital infrastructure.
2. Culturally responsive K–12 cybersecurity education.
3. The program should provide reduced certification costs and mentoring services to minorities through subsidized initiatives.
4. The development of inclusion as an essential element for cybersecurity readiness should become the focus of new policies.

Organizations need to reform their hiring processes in order to validate employment qualifications from alternative career routes. An inclusive cybersecurity ecosystem grows both the economy and the capacity for national strength. Addressing this digital civil rights issue requires educators and policymakers to work alongside business leaders to streamline their efforts. More research should be directed toward understanding the career advancement processes of the minority groups who pursue a course in cybersecurity. Longitudinal research studies would increase knowledge about the factors that enable or hinder career progression in cybersecurity—through examining workflows over an extended period. The evaluation of specific workforce development strategies, including community-based cybersecurity teaching and subsidized certification programs, aims to analyze their effectiveness in enhancing workforce diversity. Subsequent studies need to analyze how public and private funding combinations can expand access to and participation in cybersecurity training programs for underrepresented populations.

Future research will investigate approaches through which K–12 schools should implement culturally sensitive cybersecurity programs for their underprivileged geographic areas. The assessment of artificial intelligence and automation tools for cybersecurity recruitment must determine how their biases could unintentionally expand digital inequality gaps. The research will provide details for developing future-oriented systems promoting an inclusive cybersecurity environment.

REFERENCES

AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, *141*, 103845.

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K. K. R. (2022). The role of national cybersecurity strategies in the improvement of cybersecurity education. *Computers & Security*, *119*, 102754.

Barile, S., Ciasullo, M. V., Testa, M., & La Sala, A. (2023). An integrated learning framework of corporate training system: a grounded theory approach. *The TQM Journal*, *35*(5), 1106-1134.

Braveman, P. A., Arkin, E., Proctor, D., Kauh, T., & Holm, N. (2022). Systemic and Structural Racism: Definitions, Examples, Health Damages, and Approaches to Dismantling: A Study examines definitions, examples, health damages, and dismantling systemic and structural racism. *Health affairs*, *41*(2), 171–178.

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917-938.

Chukwurah, N., Abieba, O. A., Ayanbode, N., Ajayi, O. O., & Ifesinachi, A. (2024). Inclusive Cybersecurity Practices in AI-Enhanced Telecommunications: A Conceptual Framework.

Crumpler, W., & Lewis, J. A. (2022). *Cybersecurity workforce gap* (p. 10). Center for Strategic and International Studies (CSIS).

Gonzalez, P. (2021). *Retaining and Supporting BIPOC Professionals in PWIs: Addressing PWIs Equity Gap* (Doctoral dissertation, University of Southern California).

Head, B. W. (2022). *Wicked problems in public policy: Understanding and responding to complex challenges* (p. 176). Springer Nature.

Huang, B. (2024). Navigating digital divide: exploring the influence of ideological and political education on cybersecurity and digital literacy amid information warfare. *Current Psychology*, *43*(28), 23815–23836.

McBride, S., Schou, C., & Slay, J. (2022, March). A Vertically Integrated Pathway for Infusing Engineering Technicians with Industrial Cybersecurity Competencies. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 9, No. 1, pp. 8-8).

Nobles, C. (2020). The cyber talent gap and cybersecurity professionalizing. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 56-63). IGI Global.

Prewitt, M. M. J. (2024). *Intersectionality and Career Persistence of African American Women in Cybersecurity Careers: A Narrative Inquiry* (Doctoral dissertation, University of Arkansas).

Salsberg, E., Richwine, C., Westergaard, S., Martinez, M. P., Oyeyemi, T., Vichare, A., & Chen, C. P. (2021). Estimation and comparison of current and future racial/ethnic representation in the US health care workforce. *JAMA network open*, *4*(3), e213789-e213789.

Shanley, D. (2021). Imagining the future through revisiting the past: the value of history in thinking about R (R) I’s possible future (s). *Journal of Responsible Innovation*, *8*(2), 234–253.

Williams, L. D. (2021). Concepts of Digital Economy and Industry 4.0 in Intelligent and information systems. *International Journal of Intelligent Networks*, *2*, 122–129.

Wongkrachang, S. (2023). Cybersecurity awareness and training programs for racial and sexual minority populations: An examination of effectiveness and best practices. *Contemporary Issues in Behavioral and Social Sciences*, *7*(1), 35-53.