

Chapter 5

Bridging the Gap: Investigating the Barriers to African American Inclusion in the Cybersecurity Workforce

Miranda Stanfield

Capitol Technology University, USA

ABSTRACT

Despite the growing demand for cybersecurity experts, African-American professionals continue to encounter significant obstacles in accessing and advancing their careers within this field. This research examines the factors contributing to this hiring gap, including educational disparities, a lack of awareness, and implicit bias. Furthermore, this chapter highlights the adverse consequences of such disparities, not only for an individual's career prospects but also for the overall diversity, innovation, and resilience of the cybersecurity ecosystem. By shedding light on these disparities, this chapter aims to contribute to the broader discourse on diversity and inclusion within the industry, encouraging positive change and ultimately fostering a more representative and robust cybersecurity workforce for the future.

INTRODUCTION

The Cybersecurity and Infrastructure Security Agency defines cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (CISA, 2021) Cybersecurity is a profession with highly trained professionals who implement the security measures required to protect an organization's information systems (Hoffman et al., 2012). As technology increasingly becomes part of our daily lives and essential systems, the importance of adept professionals safeguarding our digital world cannot be overstated. Cybersecurity experts protect against cyber threats, safeguarding sensitive information, national security, and privacy. The cybersecurity community continues to face a significant underrepresentation of African-American professionals. The employment disparity in cybersecurity extends beyond personal career paths and significantly impacts the digital landscape's overall security. Acknowledging

DOI: 10.4018/979-8-3693-3226-9.ch005

the seriousness of this issue and devoting ourselves to comprehending its complex root causes is crucial. To effectively combat the rise of cyber threats, the cybersecurity workforce must comprise individuals from diverse backgrounds, bringing various perspectives, skills, and experiences to the field. Diversity in cybersecurity is not just a matter of social justice and equity but also a strategic necessity. Diverse teams are more adept at identifying novel threats, devising innovative solutions, and mitigating risks effectively. This underrepresentation is not merely an issue of numbers; it is a reflection of barriers that hinder the full participation of a talented and untapped pool of individuals in a field of critical importance.

Statement of the Problem

The lack of representation of minorities in the field of cybersecurity is attributed to multiple factors, such as insufficient access to education and training opportunities, limited awareness of cybersecurity careers, and perceived discrimination within the industry. (Muñoz, King, and Anderson, 2020) African Americans are underrepresented in the cybersecurity industry, with only 3.2% of the workforce comprising this group and only 12.6% of the general population. (Hale and Colbert, 2020) The general business problem statement is that the lack of African Americans in cybersecurity results in a narrow approach to tackling complex cybersecurity challenges, which could lead to national security issues or financial loss. The specific business problem is insufficient research to understand the root cause and factors surrounding the hiring gap within the U.S. cybersecurity field, specifically for Black Americans.

The Nature of the Study

Fostering a more fair and diverse hiring atmosphere in cybersecurity is critical to building a strong and effective workforce that can address the complex challenges of the digital age. Identifying and eliminating obstacles that prevent African-American cybersecurity experts from accessing job opportunities and advancing their careers is essential. This research utilized a literature review method to investigate the factors contributing to the gap in cybersecurity employment for African-American professionals. This literature examines the hiring disparities African-American professionals face in cybersecurity, highlighting the barriers they encounter and pathways toward solutions. This study aims to create a comprehensive framework that private and government industry leaders can use to promote diversity among African Americans in cybersecurity. In addition, the article intends to investigate practical approaches and recommended techniques that cybersecurity organizations can implement to foster a more fair and diverse hiring atmosphere, eliminate obstacles, and support African-American cybersecurity experts.

Methodology for the Systematic Literature Review

A literature search on the hiring gap within the cybersecurity workforce in the United States was conducted using Capitol Technology University's virtual library resources. This literature review utilized academic databases to gather relevant scholarly publications for the current study. The literature is sourced mainly from four databases EBSCOHost, IEEE Xplore, ScienceDirect, ProQuest, and Google Scholar. These databases offer access to a broad spectrum of peer-reviewed journals, conference proceedings, and books in computer science, information technology, gender studies, and organizational behavior.

In addressing the hiring gap for Blacks in the cybersecurity workforce, employing the methodological framework developed by Arksey and O'Malley (2005) offers a comprehensive approach to scoping the

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/bridging-the-gap/340568

Related Content

Diabetic Analysis and Prediction Using Deep Learning

B. Narendra Kumar Rao, Ambati Poojitha, Achyutha Guru Preethi, Aithepalli Suresh Lalith Srinivasand Buthuru Venkata Kiran Kumar Reddy (2024). *AI-Driven Innovations in Digital Healthcare: Emerging Trends, Challenges, and Applications* (pp. 211-225).

www.irma-international.org/chapter/diabetic-analysis-and-prediction-using-deep-learning/338983

Domestic Violence Is a Significant Public Health and a Health Administration Issue in the U.S.

Allison J. Huff, Darrell Norman Burrell, Amalisha Sabie Aridiand Grace E. McGrath (2023). *International Journal of Health Systems and Translational Medicine* (pp. 1-21).

www.irma-international.org/article/domestic-violence-is-a-significant-public-health-and-a-health-administration-issue-in-the-us/315298

A Survey of Unsupervised Learning in Medical Image Registration

Xin Songand Huan Yang (2022). *International Journal of Health Systems and Translational Medicine* (pp. 1-7).

www.irma-international.org/article/a-survey-of-unsupervised-learning-in-medical-image-registration/282701

Organizational Development Focused on Improving Job Satisfaction for Healthcare Organizations With Pharmacists

Amalisha Sabie Aridi, Darrell Norman Burrelland Kevin Richardson (2023). *International Journal of Health Systems and Translational Medicine* (pp. 1-15).

www.irma-international.org/article/organizational-development-focused-on-improving-job-satisfaction-for-healthcare-organizations-with-pharmacists/315297

Research on multi-view clustering algorithm on epileptic EEG signal

(2022). *International Journal of Health Systems and Translational Medicine* (pp. 0-0).

www.irma-international.org/article//282682