Building a Cybersecurity Faculty Network for HBCUs: A Collaborative Approach to Curriculum Development and Professional Growth

Marcus Isaiah Brumfield[1], Demetria White[2]

Tougaloo College, United States[1, 2]

Abstract

Historically Black Colleges and Universities (HBCUs) face growing pressure to develop robust cybersecurity programs despite faculty knowledge and expertise due to resource limitations, training opportunities, and funding limitations. This paper proposes the creation of a collaborative faculty network specifically designed to support cybersecurity educators at HBCUs. The network would be a centralized platform for faculty to access and exchange curated teaching materials, sample syllabi, certification study guides, and hands-on lab resources. It would also foster peer mentorship and connect faculty with cybersecurity professionals and organizations to help guide curriculum development and industry-aligned training. In addition to professional community-building, the network would promote a "train-the-trainer" model by offering pathways for faculty to engage in free or low-cost online courses and virtual environments such as Cisco Packet Tracer and Hack The Box. This experience-based proposal aims to strengthen HBCU cybersecurity programs by enriching faculty expertise, aligning student learning outcomes with workforce needs, and increasing academic and career-building opportunities. Through this initiative, HBCUs can create a sustainable, community-driven solution that elevates educator capacity and student success in cybersecurity.

Keywords: *HBCUs, cybersecurity education, faculty development, curriculum collaboration, online learning, professional networks*

1. Introduction

Cybersecurity job vacancies in the United States totaled 457,433 from September 2023 to August 2024, with only 83 qualified professionals for every 100 openings [11]. One way to address this is by expanding cybersecurity education to more institutions. Historically Black Colleges and Universities (HBCUs) are important in increasing access to higher education and diversifying the nation's workforce. Even with this, these institutions face persistent challenges in developing robust cybersecurity programs. As the demand for cybersecurity professionals grows, HBCUs encounter significant hurdles, such as limited faculty resources, funding constraints, and a scarcity of specialized training opportunities. Challenges such as these impede their ability to build and sustain competitive curricula. Additionally, the rapid evolution of cyber threats and the increasing complexity of skills required by industry make it difficult for faculty to stay current and for students to gain hands-on experience aligned with workforce needs [15].

Despite these obstacles, HBCUs have demonstrated resilience and innovation, with several institutions earning Centers of Academic Excellence (CAE) designations and participating in collaborative initiatives such as the Consortium of Cybersecurity Clinics. However, the lack of a centralized support system for faculty remains a critical gap. Faculty often work in isolation, with limited opportunities to share resources, access professional development, or connect with industry partners [3].

This paper suggests establishing a collaborative cybersecurity faculty network designed explicitly for HBCUs, but it applies to any educational institution or organization. The network aims to address existing gaps by providing a centralized platform for resource-sharing, peer mentorship, and industry engagement. By implementing a community-driven approach, the goal involves strengthening faculty expertise, enhancing curriculum development, and improving student outcomes in cybersecurity. HBCUs can collectively elevate their capacity to prepare the next generation of cybersecurity professionals through shared resources, professional growth opportunities, and strategic partnerships.

2. Background

2.1 State of Cybersecurity Programs at HBCUs

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, sponsored by the National Security Agency (NSA), sets the national standard for excellence in cybersecurity education and workforce preparation [16]. Institutions can meet this standard through a rigorous process that assesses curriculum, faculty expertise, institutional support, and student engagement. The NCAE-C accreditation shows the commitment to producing the next generation of cybersecurity professionals [28]. There are three primary NCAE-C designations:

- CAE in Cyber Defense (CAE-CD): This distinction recognizes institutions with robust programs in cyber defense education, emphasizing curriculum aligned with national standards, hands-on learning, and workforce readiness.
- CAE in Cyber Operations (CAE-CO): This distinction focuses on institutions offering advanced, technically deep programs in cyber operations, including offensive and defensive techniques, critical infrastructure protection, and applied research.
- CAE in Research (CAE-R): This distinction highlights institutions significantly contributing to cybersecurity research, fostering innovation and knowledge creation.

These designations serve as benchmarks for cybersecurity programs that are highly regarded by employers, government agencies, and industry partners as high standards.

Despite the importance of these designations, HBCUs remain underrepresented. For CAE-designated institutions, only 13 are HBCUs, accounting for just 2.7% of the total 475 institutions [16]. Greater support and targeted initiatives are needed to increase HBCU participation in nationally recognized cybersecurity education and research. There are opportunities for HBCUs to work towards expanding cybersecurity education and workforce development with collaboration, resource-sharing, and strategic investments [17].

The Consortium of Cybersecurity Clinics offers an innovative and community-centered approach to advancing cybersecurity education and workforce development [5]. Unlike traditional academic pathways, the consortium brings together higher education institutions nationwide to operate cybersecurity clinics that provide real-world services to local organizations, nonprofits, and municipalities. These clinics enable students to gain hands-on experience by working directly on cybersecurity projects that address community needs [9]. At the same time, faculty benefit from collaborative curriculum development and professional engagement with peers across the country.

Participation in the Consortium of Cybersecurity Clinics provides HBCUs and other institutions with an alternative route to building cybersecurity capacity and fostering community among educators, students, and industry partners. The consortium emphasizes experiential learning, mentorship, and community impact, helping to bridge the gap between academic preparation and workforce demands. As of 2024, there are only four (4) HBCUs out of 18 total active clinics of the consortium, which accounts for 22.2% of the total. The consortium reflects the growing interest in this collaborative, service-oriented model as a complement or alternative to traditional NCAE-C pathways [5].

While the presence of HBCUs in nationally recognized cybersecurity initiatives such as the NCAE-C program and the Consortium of Cybersecurity Clinics demonstrates progress, these numbers also reveal a need to increase representation and access to resources. The ongoing structural and institutional challenges limit HBCUs' participation in these programs, highlighting the need to address these issues to ensure growth and impact in the cybersecurity education landscape. The following section explores the barriers HBCUs face in expanding and sustaining high-quality cybersecurity programs, underscoring the need for collaborative, community-driven solutions.

2.2 Challenges

The funding and endowment disparities facing HBCUs stem from a legacy of systemic underinvestment, primarily due to state and federal policies. HBCUs have historically received less public funding through inequitable land-grant allocations and insufficient state matching, resulting in endowment gaps where public HBCUs average $7,265 per student compared to $25,390 at public non-HBCUs [20, 23]. Historically, HBCUs have had limited access to high-yield investment opportunities and fewer resources to allocate towards professional endowment management, which further restricts their financial growth [18]. The aforementioned challenges lead most HBCUs to rely more heavily on tuition and government funding, directly impacting their capacity to invest in faculty, infrastructure, and innovative programs such as cybersecurity.

Implementing and sustaining cybersecurity programs at HBCUs has a range of persistent challenges. Limited funding to support recruitment, lab infrastructure, and the latest technological resources is one of the primary reasons [10]. Many HBCUs operate with smaller endowments and fewer financial reserves than larger institutions, such as research institutions designated by the Carnegie Classification of Institutions of Higher Education, making it challenging to maintain cybersecurity programs and curricula [6].

Faculty shortages further complicate these efforts due to the limited availability of educators with specialized cybersecurity expertise. This shortage limits the availability of course offerings, student mentorship, and workforce preparation [1, 2]. Professional development opportunities for faculty are also limited, with few resources dedicated to ongoing training and certification in emerging cybersecurity fields [15].

Resource gaps are another significant barrier. Many HBCUs lack access to hands-on labs, industry-aligned training tools, and current teaching materials. Due to the lack of resources, experiential learning and aligning the curriculum with workforce needs are more challenging to implement. Additionally, cybersecurity threats and compliance requirements present ongoing risks [17].

Lastly, workforce alignment remains a challenge. University curricula often lag behind the rapidly evolving industry demands and certification requirements, making it difficult for graduates to compete for high-demand cybersecurity roles. Broader and sustained support is needed to close persistent gaps in cybersecurity education at HBCUs [10].

2.3 Case Studies and Best Practices

Successful faculty networks and collaborative initiatives in STEM and cybersecurity provide valuable models for HBCUs seeking to strengthen their programs and professional networks. Below are examples of such networks and programs, each offering unique strategies for faculty development, curriculum enhancement, and workforce preparation.

Case Study 1: The Center for Equitable AI and Machine Learning Systems (CEAMLS) at Morgan State University is an interdisciplinary hub dedicated to advancing equitable and socially responsible AI and machine learning systems. The center supports K-12 STEM education, faculty research, and professional development, emphasizing the reduction of algorithmic bias and developing a diverse next-generation STEM workforce. CEAMLS also hosts national symposia, collaborates on inclusive AI projects, and provides resources for both educators and students to engage with emerging technologies in a fair and unbiased manner [4, 14].

Case Study 2: The Coding School is a nonprofit organization focused on building workforce skills in emerging technologies, including AI and machine learning. It offers professional development for educators, such as hands-on workshops and sessions on integrating AI into classroom instruction. These initiatives equip faculty with the knowledge and tools to teach and apply AI responsibly, while supporting faculty growth and student learning outcomes [28].

Case Study 3: The HBCU Faculty Fellows Program from PROPEL empowers faculty through transformative professional development to improve student outcomes. The program features a curriculum co-designed by industry experts and HBCU faculty, emphasizing active learning, digital resilience, and technology integration. Faculty benefit from mentorship, leadership development, and collaboration with peers and industry partners, enhancing instructional practices and student engagement [27].

Case Study 4: Mississippi Artificial Intelligence Network (MAIN) is the nation's first and only statewide AI network, connecting K-12 schools, community colleges, universities, businesses, and industry partners in Mississippi. MAIN delivers free AI courses, workforce training, and technical expertise, making AI education accessible nationwide. The network's partnerships with organizations like Intel, Amazon Web Services, and NVIDIA strengthen its impact, providing scalable models for faculty and instructor development in AI and cybersecurity [12].

Case Study 5: The Mississippi Cyber Initiative, led by Mississippi State University, provides statewide leadership in preparing Mississippi’s future workforce and economy through digital collaboration and innovation. MCI partners with state, federal, and industry partners to address cybersecurity training needs, support economic development, and deliver timely workforce training. The initiative spreads digital and cyber knowledge to students, faculty, small businesses, and industry across Mississippi, focusing on K-12 outreach, higher education, and professional development. MCI operates a cyber ecosystem for hands-on training, launches a digital forensics lab for law enforcement, and hosts summits and tabletop exercises to foster collaboration and innovation [13].

These case studies demonstrate the importance of faculty networks, cross-sector partnerships, and targeted professional development in building resilient and innovative cybersecurity and STEM programs. By adopting and adapting these best practices, HBCUs can enhance faculty expertise, improve student outcomes, and contribute meaningfully to the national cybersecurity workforce.

3. Proposed Model

The proposed model involves a cybersecurity faculty network for HBCUs. Based on educational research and successful case studies, the proposed faculty network can integrate methodologies such as collaborative learning theory, peer mentoring frameworks, and structured curriculum development models to create a sustainable, community-driven platform. Below is a recommended approach based on the literature and existing best practices.

The collaborative learning theory originates from Vygotsky's constructivist framework, which connects to social constructivism (i.e., the active construction of knowledge through education as a direct result of social interaction and collaboration) [26]. The network's design aligns with collaborative learning theory, emphasizing knowledge construction through social interaction, shared responsibility, and diverse perspectives [8, 27]. By fostering peer-to-peer (P2P) engagement, the network can enhance faculty motivation and self-efficacy through shared experiences and co-creation of resources, reduce isolation by building relational connections among HBCU faculty, similar to the benefits observed in PhD mentoring programs, and improve curriculum alignment with workforce needs by leveraging collective expertise, as seen in the Cyber-HAWKS Peer Mentoring Program [7].

To effectively guide faculty development and resource integration, the network should adopt a hybrid curriculum design model that blends Tyler's [28] objectives-based approach with Taba's [27] interactive model. This approach allows for pre-defined goals (e.g., certification readiness) and dynamic feedback loops (e.g., faculty-driven resource needs). Table 1 outlines a phased model for implementing the network, each phase grounded in educational design principles and practical implementation strategies.

Table 1. This table provides a template for the key phases and actions for the proposed model to support collaborative curriculum development and peer mentoring for cybersecurity education.

Phase	Action	Example Implementation
Initial Assessment	Take a look at faculty and program needs (curricula, course syllabi, course/lab resources)	Conduct surveys or focus groups to identify areas of need (e.g., faculty development, low-cost resources).
Objective Setting	Establish learning outcomes for faculty (certification readiness, curriculum development, outreach)	Develop a plan of action based on the respective faculty's needs.
Content Selection	Gather open-access resources	Integrate free/low-cost material such as CISA learning modules, Cisco Packet Tracer, HackTheBox labs, etc.
Implementation	Provide peer-led workshops, resources tailored to specific courses, and access to peer mentors.	Monthly virtual seminars, bi-monthly meetings with peer mentors, open access to example syllabi and workshop templates

Evaluation	Measure impacts such as faculty retention, certification rates, and student outcomes.	Use pre/post-surveys and longitudinal tracking of student workforce placement.

This phased model integrates established educational theories with practical implementation strategies to direct cybersecurity faculty through structured collaboration, shared resources, and professional development. This program tailors its approach to meet the needs of HBCUs but can adapt to cybersecurity education across various institutions and organizations. Peer mentoring, open-access content, and curriculum alignment make it suitable for settings with limited resources but high potential impact [28]. The model's expected outcomes include faculty growth, student success, and increased institutional capacity in cybersecurity education.

5. Expected Outcomes and Impact

Implementing the proposed cybersecurity faculty network model will generate significant and measurable benefits for faculty, students, and institutions. For faculty, the network fosters professional growth through certification readiness support, access to teaching materials, and engagement with peers and industry professionals. This model improves faculty confidence and instructional effectiveness and supports long-term retention by reducing isolation and burnout, common challenges in under-resourced programs [27].

Students experience indirect benefits through improved course quality, more consistent integration of hands-on labs and simulations, and stronger alignment with industry certifications and career pathways [27]. As instructors incorporate updated materials, tools like Cisco Packet Tracer and Hack The Box, and real-world case studies into the curriculum, students are more likely to graduate with job-ready skills and a clearer understanding of cybersecurity roles. Faculty who receive regular support have a better impact on mentoring students, facilitating certification prep, and connecting students with internships or entry-level opportunities [27].

At the institutional level, participation in the network strengthens overall program quality and competitiveness. It supports grant-readiness by demonstrating collaborative efforts and professional development initiatives, and it lays the groundwork for future designations such as Centers of Academic Excellence (CAE) or inclusion in national consortia. Additionally, the shared resources and scalable framework allow institutions to lower the cost of curriculum development and faculty onboarding, enabling even smaller or emerging programs to build sustainable cybersecurity pathways.

The proposed model helps expand cybersecurity education by providing faculty at HBCUs and similarly under-resourced institutions with the tools and community necessary to build high-impact, workforce-aligned programs. The flexible design may be implemented at various institutional scales to diversify and expand the cybersecurity workforce.

7. Conclusion

Addressing the growing demand for cybersecurity professionals requires intentional investment in faculty development, curriculum innovation, and collaborative infrastructure. This is especially true at institutions like HBCUs, which play a critical role in diversifying the workforce. This paper proposes a scalable faculty network model to support educators through resource sharing, peer mentorship, and access to hands-on training tools. The network empowers faculty to build stronger, more aligned cybersecurity programs that benefit students and institutions by lowering barriers to instructional quality and professional growth.

Educational leaders, grant-making organizations, and industry partners are encouraged to support the launch and expansion of this network. Through collective action, the national cybersecurity pipeline ensures that all institutions, regardless of size or funding, have the opportunity to contribute to a more secure digital future.

REFERENCES

[1] Anderson, D., & Reimers, K. (2019). Cyber security employment policy and workplace demand in the US government. In *EDULEARN19 Proceedings* (pp. 7858–7866). IATED.

[2] Angelique, H., Kyle, K., & Taylor, E. (2002). Mentors and muses: New strategies for academic success. *Innovative Higher Education, 26*(3), 195–209. https://doi.org/10.1023/A:1017968906264

[3] Burrell, D. N., & Webber, C. D. (2024). Why historically black colleges and universities (HBCUs) should employ new approaches to cybersecurity faculty development. In *Evolution of Cross-Sector Cyber Intelligent Markets* (pp. 378–395). IGI Global Scientific Publishing.

[4] Center for Equitable Artificial Intelligence and Machine Learning Systems. (n.d.). https://www.morgan.edu/ceamls

[5] Consortium of Cybersecurity Clinics. (2025). *Cybersecurity for the public good*. https://cybersecurityclinics.org/

[6] Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024, March). A critical review of cybersecurity education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (pp. 241–247).

[7] Dodge, E. N., Fish, R. E., & Thompson, J. R. (2021). Fostering faculty development through peer mentoring: A model from Cyber-HAWKS. *Journal of Cybersecurity Education, Research and Practice, 2021*(1). https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/2

[8] Dooly, M. (2008). Constructing knowledge together. In M. Dooly (Ed.), *Telecollaborative language learning: A guidebook to moderating intercultural collaboration online* (pp. 21–45). Peter Lang.

[9] Google.org. (2024). *Google cybersecurity investments: Supporting HBCUs and training programs*. https://blog.google/outreach-initiatives/google-org/google-cybersecurity-investments-june-2024/

[10] Hart, P. (2024). Improving HBCU cybersecurity programs to build a capable workforce. *Forbes Technology Council*. https://www.forbes.com/councils/forbestechcouncil/2024/04/30/improving-hbcu-cybersecurity-programs-to-build-a-capable-workforce/

[11] Hozza, D. (2024). Entering the cybersecurity workforce: Certification vs. college degree. In *Innovative Practices in Teaching Information Sciences and Technology: Further Experience Reports and Reflections* (pp. 221–230). Springer Nature Switzerland.

[12] Mississippi Artificial Intelligence Network. (n.d.). https://www.sreb.org/ai-main

[13] Mississippi Cyber Initiative. (n.d.). https://www.mscyberinitiative.org/

[14] Morgan’s Center for Equitable AI and Machine Learning Systems to test efficacy and functionality of new inclusive large language model AI. (n.d.). https://www.morgan.edu/news/ceamls-to-test-large-language-model-ai

[15] Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, 157–176.

[16] National Centers of Academic Excellence in Cybersecurity. (n.d.). *CAE institution map*. Retrieved May 24, 2025, from https://www.caecommunity.org/cae-map

[17] Namukasa, M., Ficke, C., & Piasecki, I. (2023). Understanding how to diversify the cybersecurity workforce: A qualitative analysis. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), 4.

[18] PGIM & UNCF. (2024, January 29). PGIM, UNCF study finds private HBCU endowments need investment support. https://www.pgim.com/us/en/institutional/about-us/newsroom/press-releases/pgim-uncf-study-finds-private-hbcu-endowments-need-investment-support

[19] PROPEL. (2024, March 14). *PROPEL, Southern Company launch HBCU-focused cybersecurity consortium*. *Access Newswire*. https://www.accessnewswire.com/newsroom/en/utilities/propel-southern-company-launch-hbcu-focused-cybersecurity-consortium-858542
[20] Smith, D. A. (2021). Achieving Financial Equity and Justice for HBCUs. *Century Foundation*.
[21] Taba, H. (1962). *Curriculum development: Theory and practice*. Harcourt Brace.
[22] The Coding School. (n.d.). https://the-cs.org/
[23] The White House. (2024, May 16). The economics of HBCUs. https://bidenwhitehouse.archives.gov/cea/written-materials/2024/05/16/the-economics-of-hbcus/
[24] Tran, B., Benson, K. C., & Jonassen, L. (2023). Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce. *Journal of Cybersecurity Education, Research and Practice, 2023*(2).
[25] Tyler, R. W. (1949). *Basic principles of curriculum and instruction*. University of Chicago Press.
[26] Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.
[27] Wagner, P. (2023). CyberEducation-by-design. *Cybersecurity Pedagogy & Practice Journal, 2832*, 1006.
[28] Weitl-Harms, S., Spanier, A., Hastings, J., & Rokusek, M. (2023). A systematic mapping study on gamification applications for undergraduate cybersecurity education. *Journal of Cybersecurity Education, Research and Practice, 2023*(1).