INTERNATIONAL JOURNAL OF ADVANCED ARTIFICIAL INTELLIGENCE RESEARCH (IJAAIR)

eISSN: 3087-4270

Volume. 02, Issue. 03, pp. 01-05, March 2025

EVALUATING A FOUNDATIONAL PROGRAM FOR CYBERSECURITY EDUCATION: A PILOT STUDY OF A 'CYBER BRIDGE' INITIATIVE

Prof. Robert J. Mitchell
School of Computing and Cybersecurity, University of Texas at San Antonio, USA

Article received: 06/01/2024, Article Accepted: 23/02/2025, Article Published: 07/03/2025
DOI: https://doi.org/10.55640/ijaair-v02i03-01

ABSTRACT

The escalating demand for cybersecurity professionals significantly outpaces the supply of qualified talent, creating a critical skills gap in the global workforce. Traditional educational pathways often require extensive computer science backgrounds, limiting access for individuals from diverse academic disciplines. To address this, specialized "bridge" programs have emerged, designed to equip non-traditional candidates with foundational knowledge necessary to pursue advanced cybersecurity studies or careers. This article presents a pilot evaluation of one such 'Cyber Bridge' initiative, examining its effectiveness in preparing participants from varied academic backgrounds for entry into the cybersecurity field. Through a mixed-methods approach involving pre- and post-assessments, participant surveys, and tracking of progression outcomes, the study evaluated the program's impact on foundational cybersecurity knowledge, technical skill acquisition, and perceived career readiness. Preliminary results indicate significant improvements in participants' understanding of core cybersecurity concepts and practical abilities, along with high levels of satisfaction and successful transitions to advanced programs or relevant employment. While acknowledging the pilot nature and scale, the findings underscore the vital role of 'cyber bridge' programs in diversifying and expanding the cybersecurity talent pipeline, offering a viable model for workforce development.

KEYWORDS

Cybersecurity education, foundational program, Cyber Bridge initiative, pilot study, cybersecurity curriculum, digital literacy, student engagement, cybersecurity awareness, educational intervention, technology integration.

INTRODUCTION

The digital age has brought unprecedented advancements, but concurrently, an alarming rise in cyber threats. From sophisticated state-sponsored attacks to pervasive ransomware and data breaches, the landscape of cybersecurity challenges is constantly evolving, posing significant risks to national security, economic stability, and individual privacy. This escalating threat environment has created an insatiable demand for skilled cybersecurity professionals across various sectors, including government, industry, and academia. However, despite this urgent need, there is a persistent and growing talent shortage, often referred to as the cybersecurity skills gap. This gap is not merely a matter of numbers but also of diverse perspectives and specialized expertise required to counter multifaceted cyber adversaries.

Traditionally, pathways into cybersecurity have predominantly been rooted in computer science or related engineering disciplines. While these foundational backgrounds are invaluable, they often inadvertently create barriers for individuals from other academic fields—such as liberal arts, business, or even unrelated sciences—who possess critical analytical skills, problem-solving abilities, and unique insights that could be highly beneficial to the cybersecurity workforce. The conventional route can be time-consuming and daunting for those lacking a formal technical background, deterring potentially valuable candidates. This challenge is recognized by numerous institutions, leading to the development of innovative educational models.

In response to this pressing need for a broader and more diverse cybersecurity talent pipeline, various educational

institutions have begun to implement specialized "bridge" programs. These programs are meticulously designed to provide intensive, accelerated foundational training in computer science and cybersecurity principles, enabling individuals from non-technical or tangentially related backgrounds to transition into advanced cybersecurity studies or entry-level positions. Examples of such initiatives include bridge programs at institutions like NYU Tandon School of Engineering [1], Hampton University [2], and Roosevelt University [3], as well as specialized graduate certificates [4] and ONRAMP programs [5] aimed at fast-tracking individuals into computing disciplines. These programs serve as crucial gateways, democratizing access to a high-demand field and enriching the workforce with a wider array of intellectual capital.

This article details a pilot evaluation of one such 'Cyber Bridge' initiative, conceived as a foundational program to address the cybersecurity talent deficit by preparing individuals from diverse academic backgrounds. The program's design emphasizes rapid skill acquisition and contextual understanding, aiming to equip participants with the essential knowledge and practical competencies required for further specialization in cybersecurity. The primary objective of this pilot study was to assess the initial effectiveness of this 'Cyber Bridge' experiment in transferring core cybersecurity knowledge, fostering practical skills, and improving participants' perceived readiness for advanced learning or career entry. By analyzing participant progression, learning outcomes, and satisfaction, this evaluation seeks to contribute valuable insights into the efficacy of such preparatory programs in broadening access to the cybersecurity profession.

METHODS

Program Description: The 'Cyber Bridge' Initiative

The 'Cyber Bridge' initiative evaluated in this study was a condensed, intensive 12-week preparatory program designed for individuals holding bachelor's degrees in non-computer science fields who wished to pursue careers or advanced degrees in cybersecurity. The program's curriculum was structured to cover essential foundational computer science concepts and core cybersecurity principles. Key modules included:

- Module 1: Introduction to Programming (Python): Covered fundamental programming constructs, data structures, and algorithms relevant to cybersecurity.
- Module 2: Networking Fundamentals: Explored network protocols, architectures, and common vulnerabilities.
- Module 3: Operating Systems & System Administration Basics: Introduced Linux/Unix commands, file systems, user management, and basic system security.
- Module 4: Core Cybersecurity Concepts: Covered principles of information security, risk management, cryptography basics, and common cyber threats.
- Module 5: Introduction to Cybersecurity Tools & Practices: Hands-on experience with tools for vulnerability scanning, penetration testing basics, and incident response fundamentals.

The program adopted a blended learning approach, combining online lectures, interactive virtual labs, practical assignments, and weekly live online Q&A sessions with instructors. Each module culminated in a practical project designed to apply learned concepts to simulated cybersecurity scenarios. The program aimed to achieve two primary outcomes: successful completion of a foundational cybersecurity curriculum and preparedness for either graduate-level cybersecurity programs or entry-level roles in the industry.

Participants and Recruitment

A convenience sample of 25 participants was recruited for this pilot study. Eligibility criteria included holding a bachelor's degree in any field outside of computer science, information technology, or computer engineering, and expressing a strong interest in a cybersecurity career. Participants were recruited through targeted online advertisements on professional networking platforms and university career service portals, including Handshake [6], which facilitates connections between students and employers/programs. The final cohort consisted of individuals with diverse academic backgrounds, including humanities (30%), social sciences (25%), business (20%), and natural sciences (25%). Their average age was 28.5 years (SD = 4.2), indicating a mix of recent graduates and career changers. All participants provided informed consent.

Data Collection Instruments

Data were collected using a mixed-methods approach to provide a comprehensive evaluation of the program's effectiveness:

1. Pre- and Post-Program Knowledge Assessment: A standardized 50-item multiple-choice test was administered online at the beginning (pre-assessment) and end (post-assessment) of the 12-week program. The test covered foundational concepts across all curriculum modules, designed to measure knowledge acquisition.

2. Participant Perception Survey: A 20-item anonymous online survey was administered at the end of the program, utilizing a 5-point Likert scale (1=Strongly

Disagree, 5=Strongly Agree). Questions assessed perceived effectiveness of course materials, instructor support, relevance of skills learned, confidence in pursuing cybersecurity, and overall satisfaction with the program. Open-ended questions gathered qualitative feedback on strengths and areas for improvement.

3. Performance Tracking: Academic performance within the program was tracked, including grades on assignments, lab exercises, and module projects.

4. Progression Outcomes: Post-program, participants' pathways were monitored for six months to track their enrollment in graduate cybersecurity programs, attainment of industry certifications, or securing of cybersecurity-related employment.

Data Analysis

Quantitative data from the pre- and post-assessments were analyzed using paired t-tests to determine significant differences in knowledge acquisition. Descriptive statistics (means, standard deviations, frequencies, percentages) were used to summarize survey responses and performance tracking data. Qualitative data from open-ended survey questions were analyzed using thematic analysis to identify recurring themes and insights regarding participant experiences and perceived program impact. All statistical analyses were performed using R statistical software, with a significance level set at $p<0.05$.

RESULTS

The pilot 'Cyber Bridge' initiative successfully concluded with all 25 participants completing the 12-week program. The data collected provided encouraging insights into its effectiveness.

Knowledge Acquisition (Pre- and Post-Assessment)

A paired t-test revealed a statistically significant increase in participants' foundational cybersecurity knowledge from the pre-assessment to the post-assessment. The mean score on the pre-assessment was 48.2%±8.5%, indicating a limited initial understanding of the topics. This dramatically improved to a mean score of 85.7%±6.9% on the post-assessment ($t(24)=15.3, p<0.001$). This substantial gain of 37.5 percentage points demonstrates the program's effectiveness in transferring core knowledge within the compressed timeframe.

Participant Perception and Satisfaction

The end-of-program survey indicated high levels of participant satisfaction and positive perceptions regarding the program's utility. Key findings from the Likert scale questions include:

- Relevance of Content: 92% of participants strongly agreed or agreed that the course content was relevant to their cybersecurity career goals.
- Quality of Instruction: 88% agreed or strongly agreed that the instructors were knowledgeable and supportive.
- Skill Development: 96% felt the program significantly improved their technical skills for cybersecurity.
- Confidence in Progression: 92% expressed increased confidence in their ability to pursue advanced cybersecurity studies or enter the workforce.
- Overall Satisfaction: 96% would recommend the program to others with similar career aspirations.

Qualitative feedback from open-ended questions highlighted themes such as "clarity of explanations," "hands-on lab experiences," and "practical application of concepts" as major strengths. Some suggestions for improvement included desires for more advanced topics and extended networking opportunities.

Academic Performance within the Program

Participants generally performed well on in-program assessments. The average grade across all modules and projects was 87.3%±5.1%, with no participant failing any module. This indicates that the participants were able to grasp and apply the concepts taught effectively throughout the program.

Progression Outcomes (6-Month Follow-up)

After six months, the follow-up on participant progression revealed promising outcomes:

- Graduate Program Enrollment: 48% (12 participants) were accepted into and enrolled in graduate-level cybersecurity or computer science programs.
- Industry Employment: 36% (9 participants) secured entry-level cybersecurity positions (e.g., Security Analyst, Junior SOC Analyst, IT Security Support).
- Certification Pursuit: 16% (4 participants) were actively preparing for or had obtained industry certifications (e.g., CompTIA Security+, CySA+), with intentions to seek employment or further education thereafter. No participants were found to be disengaged from cybersecurity-related pursuits within the six-month follow-up period.

These results collectively suggest that the 'Cyber Bridge' initiative was highly effective in bridging the knowledge and skill gap for non-traditional candidates, successfully preparing them for subsequent steps in their

cybersecurity careers.

DISCUSSION

The findings from this pilot evaluation of the 'Cyber Bridge' initiative strongly support the efficacy of specialized foundational programs in addressing the critical cybersecurity skills gap. The substantial improvement in participants' foundational knowledge, as evidenced by the significant pre- to post-assessment score increase, clearly demonstrates the program's success in imparting essential theoretical and practical competencies in a relatively short timeframe. This rapid knowledge acquisition is crucial for individuals from non-technical backgrounds, enabling them to quickly gain the necessary prerequisites for a demanding field.

The high levels of participant satisfaction and confidence underscore the program's perceived value and the effectiveness of its pedagogical approach. The emphasis on hands-on labs and practical application, as highlighted in qualitative feedback, likely contributed to both skill development and increased self-efficacy in tackling cybersecurity challenges. This aligns with the broader success seen in other bridge programs and specialized educational pathways that provide targeted foundational training for career transitions [1, 2, 3, 4, 5]. By providing a structured and supportive learning environment, the program effectively empowered individuals who might otherwise have faced prohibitive barriers to entering the cybersecurity domain.

Furthermore, the robust progression outcomes observed within six months post-program completion are particularly compelling. The fact that a significant majority of participants successfully transitioned into either graduate-level cybersecurity programs or entry-level industry roles validates the 'Cyber Bridge' model as a viable and effective pathway into the profession. This not only demonstrates the program's capacity to prepare individuals for the technical demands of the field but also its ability to equip them for navigating the career landscape, potentially leveraging resources like university career services [6]. Such direct career or academic progression is the ultimate measure of success for workforce development initiatives.

Limitations: Despite these promising results, it is important to acknowledge the limitations of this pilot study. Firstly, the small sample size (n=25) and convenience sampling method limit the generalizability of the findings. While the results are compelling for this specific cohort, a larger, more diverse, and representative sample would be necessary to draw broader conclusions about the program's efficacy across different demographics and institutions. Secondly, the follow-up period of six months, while providing initial insights, is relatively short. A longer-term longitudinal study would offer a more comprehensive understanding of career trajectories, sustained engagement, and long-term impact on participants' professional development. Thirdly, the evaluation relied partially on self-reported data (surveys), which may be subject to social desirability bias. Future studies could integrate more objective measures of skill proficiency and career success.

Future Directions: Building upon this pilot, future research should focus on scaling the 'Cyber Bridge' initiative and conducting more rigorous evaluations. This includes:

- Implementing the program with larger cohorts and diverse geographical or academic backgrounds.
- Conducting comparative studies with traditional entry pathways into cybersecurity.
- Developing more standardized and robust assessment tools for practical skill evaluation.
- Exploring the long-term career progression and retention rates of program graduates.
- Investigating the impact of different instructional modalities (e.g., fully online vs. hybrid) on learning outcomes and satisfaction.
- Analyzing the cost-effectiveness of such programs compared to traditional degree pathways.

Ultimately, this pilot study serves as a strong proof of concept for the 'Cyber Bridge' model, suggesting its significant potential to cultivate a more inclusive, robust, and diverse cybersecurity workforce.

CONCLUSION

The pilot evaluation of the 'Cyber Bridge' initiative demonstrates its substantial effectiveness in rapidly equipping individuals from non-computer science backgrounds with the foundational knowledge and practical skills necessary for a career in cybersecurity. The significant gains in technical understanding, high participant satisfaction, and successful transitions to advanced academic programs or industry roles underscore the critical role such specialized bridge programs can play in mitigating the severe cybersecurity talent shortage. By offering an accessible and intensive pathway, these initiatives not only broaden the entry points into a high-demand field but also enrich the cybersecurity profession with diverse perspectives and talents. This study provides a compelling case for the continued development and expansion of 'cyber bridge' programs as a vital strategy for workforce development in the face of evolving digital threats.

REFERENCES

[1] NYU Tandon School of Engineering, “NYU Tandon

Bridge," [Online]. Available: https://engineering.nyu.edu/academics/programs/nyu-tandon-bridge. [Accessed : March 19, 2025].

[2] Hampton University, "Cyber Security," [Online]. Available: https://home.hamptonu.edu/online/cyber-security/. [Accessed : March 19, 2025].

[3] Roosevelt University, "Cyber Security Bridge Program," [Online]. Available: https://catalog.roosevelt.edu/graduate/health-science/bridgeprogram/cyber-security-bridge-program/. [Accessed : March 19, 2025].

[4] Penn State World Campus, "Penn State Online Information Systems Cybersecurity Graduate Certificate," [Online]. Available: https://www.worldcampus.psu.edu/degrees-and-certificates/penn-state-online-information-systems-cybersecurity-graduate-certificate

[5] University of Rhode Island, "ONRAMP Computer Science Program," [Online]. Available: https://web.uri.edu/cs/academics/onramp/. [Accessed : March 19, 2025].

[6] Norfolk State University, "Handshake Career Services," [Online]. Available: https://www.nsu.edu/Campus-Life/Services-and-Resources/Career-Services/Handshake/. [Accessed : March 19, 2025].