ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity

MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #38251

Cybersecurity for Everybody - A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum

Nikunja Swain (Professor and Chair)

Cybersecurity for Everybody - A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum.

Abstract

Almost every career encompasses some form of security and today's students must be introduced to various aspects of security to be effective in their career and daily lives. South Carolina State University (SC State University) has an ongoing Target Infusion Proposal grant from National Science Foundation (NSF) to address the problem of the lack of awareness and participation in cyber security since 2019. The project vision is to create a successful model of institution wide reform for undergraduate cybersecurity education at SC State University using instruction, internships, and seminars. The student should be able to evaluate, make decisions, and take responsible actions in the context of cyber security.

This project uses a multi-tier approach to increase capacity in cyber security education, training, and awareness in the undergraduate curriculum The objective of this poster presentation is to share our experiences with various project activities. The findings presented in this paper may be used by interested parties involved in STEM curriculum.

Introduction

Experts agree that there is a growing need for cybersecurity professionals and universities across the country haven't caught up to the needs of the corporations. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of Cybersecurity is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. Universities are only beginning to catch up [1, 2].

Security programs, security tracks and certificates in information security exist, but often these courses are available only for computer science majors or majors in computer related disciplines [3]. Breaches in cyber infrastructure impact everyone, not just computing professionals. It is crucial that more undergraduate majors receive education and training that deepens their conceptual and practical understanding of issues in Cybersecurity [4, 5]. Professionals in the field consider it imperative for academic institutions to increase course development in computer security to make students both knowledgeable and technologically prepared for future challenges in this field. As a result, we should all recognize the importance of cybersecurity in the undergraduate curriculum. Our graduates must have security skills in addition to communication, critical thinking, and analytical skills. This additional skill will offer our majors the opportunity to extend the security focus beyond the departments, to raise awareness outside of the computer science community, and provide a path for further studies and employment in Cybersecurity [4-30].

This NSF grant project addresses this problem of the lack of awareness and participation in Cybersecurity using a multi-tier approach to increase capacity in cybersecurity education, training, and awareness in the undergraduate curriculum by creating a successful model of Cybersecurity education; and this reform will be based on our prior experience with the introduction of innovative teaching modules in a number of science, mathematics, and engineering Technology courses, faculty student seminar series, working in teams, use of simulation and K-17 student competitions.

Goals and Objectives

The goals and objectives of this project are the following:

Goal 1:Formulate a project advisory team.

Objective 1.1: Assemble a diverse team consisting of at least 5 leaders from academia and industry with experience and expertise in various aspects of Cybersecurity education.

Goal 2: Develop Cybersecurity educational material for all undergraduate majors at the University.

Objective 2.1: Develop an introductory cybersecurity course for all non-majors.

Objective 2.2: Develop course syllabus and instructional material for this course.

Objective 2.3: Get the course officially approved by the University and offer course.

Objective 2.4 Perform periodical course evaluations and use the result of the evaluations for continuous improvement.

Goal 3: Conduct Cybersecurity professional development activities for faculty, and students.

Objective 3.1: Schedule basic Cybersecurity hands-on activities for students, faculty, and community members.

Goal 4: Conduct Cybersecurity awareness activities for the students, faculty and community.

Objective 4.1: Schedule speaker series on cybersecurity for students, faculty, and community members.

Objective 4.2: Perform periodical visits to local K-17 schools to discuss various aspect of Cybersecurity.

Goal 5: Create an online space for sharing of information.

Objective 5.1: Develop a website.

Objective 5.2: Announce date and time project activities.

Objective 5.3: Share course modules with interested parties.

Anticipated Benefits

The following are some of the anticipated benefits of this project to STEM education and research at the South Carolina State University:

1. Enhanced collaboration with academia and industry can be used for various STEM educational activities.

2. Enhanced cybersecurity experience for all undergraduate majors at SC State University and surrounding academic institutions.

3. Enhanced Faculty expertise in Cybersecurity.

4. Enhanced community Cybersecurity awareness.

5. A feeder program for graduate schools and employers.

6. Improved outreach activities with K-17 institutions.

Project Findings

Goal 1: Formulated a project advisory team – We formulated the Advisory committee consisting of members of Industry, Academia and Industry professionals from Ishpi Information Technologies, Savannah River Nuclear Lab, CapGemini in Columbia, US Navy/SPAWAR, Felton Laboratory Charter School, and South Carolina State University Conducted the first meeting virtually and shared progress with the committee.

Goal 2: Develop Cybersecurity educational material for all undergraduate majors at the University - We developed a cybersecurity minor titled "Cybersecurity for all" for all majors at our university. This minor consists of six (6) cybersecurity courses with a total of 18 credit hours. The courses are:

1. Fundamentals of Cybersecurity,
2. Fundamentals of Digital Forensics,
3. Introduction to Management of Information Cybersecurity,
4. Introduction to Legal and Ethical Issues in Cybersecurity,
5. Special Topics in Cybersecurity,
6. Senior (Capstone) project in Cybersecurity

We offered two cybersecurity courses for all non-Computer Science (CS) majors at the university during 2020-21 academic year with very low enrollment. At this moment, we have only three students pursuing this Cybersecurity for All minor. We are working with various department chairs and college deans and we expect this enrollment to grow. Also, we offered all courses for our cybersecurity concentration for CS majors, and currently approximately 30 students pursuing the Cybersecurity concentration. Also, we have graduated 15 students from this concentration.

Goal 3: Conduct Cybersecurity professional development activities for faculty, and students - Building upon our successful HBCU Cybersecurity Workforce Summit for academia and industry on February

12, 2020, we formulated a consortium of the South Carolina HBCUs to develop a Degree Apprentice Program with local employers for CS/IT students at these HBCUs. Three CS/Cybersecurity faculty completed IBM Data Science Practitioner course and certified as IBM Data Science Instructors. We also offered a Data Science course for our CS/Cybersecurity majors with IBM Data Science Platform and course material, and three of the students in this course completed an IBM Data Science Exam successfully and received IBM Data Science Token.

Goal 4: Conduct Cybersecurity awareness activities for the students, faculty, and community
The Degree Apprenticeship Program mentioned in Goal 3 is developed collaboratively with Urban Institute and Ishiip, Inc. and registered with the Department of Labor. We have one employer signed into this initiative and we are in the process of recruiting more employers to this initiative. Computer Science/Cybersecurity/IT undergraduate students from consortia schools are being recruited to this degree apprentice program with an anticipated start date of Summer 2022. This degree aimed at providing the CS/IT graduates with real world skills in CS/cybersecurity in secure software development. In addition to this, we established a IC CAE and Cybersecurity Student Club at South Carolina State University and recruited 10 students to this club; encouraged students to participate cybersecurity competitions and 10 students participated in the National Cyber League (NCL) competition, and encouraged students to participate in presentation activities and 2 students presented in the IC CAE Virtual Event hosted by University of North Carolina at Charlotte, and 10 students participated in various IC CAE virtual presentations.

Goal 5: Create an online space for sharing of information - This work is on-going.

Summary and Conclusions

As seen in the project findings section, we were able to meet the project goals. We have offered The project activities were evaluated by an external evaluator and the evaluation results were shared with the advisory council and the project team. Changes to assessment activities were made based on the evaluation results as needed.

We are in year 3 of this project and we will continue executing the project goals and other activities. We plan to present the final findings of the project in another NSF poster session.

Acknowledgement

Current funding for this project has been provided by the National Science Foundation through awards – award number HRD-1912085, and award number HRD 1912284. Additional resources were provided by SC State University. The author wish to acknowledge and thank NSF and SC State University for this grant support.

References

[1]. Top U.S Universities failing at Cybersecurity Education. Retrieved from https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html

[2]. D. Rowe, B. Lunt, J. Ekstorm, "The Role of Cyber-Security in Information Technology Education" - *SIGITE'11*, October 20–22, 2011. 3

[3]. G. Meiselwitz, Information Security across Disciplines - *SIGITE'08*, October 16-18, Cincinnati, Ohio, USA.

[4]. L. Clinton (2009). "Education's Critical Role in Cybersecurity" - *EDUCAUSE Review,* vol. 44, no. 5, 60–61.

[5]. R. Raj, S. Mishra, C. Romanowski, T. Howles (2008), "CyberSecurity as General Education", 15th Colloquium for Information Systems Security Education (CISSE 2011), Fairborn, Ohio, June 2011.

[6]. Cybersecurity Curricula 2017 [Online].Available: http://www.ncsl.org/documents/taskforces/CSEC_Overview.pdf

[7]. Cybersecurity for Everyone, Not Just the IT Department [Online]. Available: http://www.ncsl.org/documents/taskforces/CompTIA_CyberSecure_Human_Error_Whitepaper.pdf

[8]. Cybersecurity: Everyone's Responsibility. [Online]. Available:

https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/C45-626825-

[9]. Cybersecurity Education and Workforce Development for the Nation, RSA Conference 2016. [online]. Available: https://www.rsaconference.com/writable/presentations/file_upload/prof-m08-cybersecurity-education-and-workforce-development-for-the-nation.pdf

[10]. NICE National Initiative for Cybersecurity education. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/National-Initiative-for-Cybersecurity-Education-(N/images-media/ispab_june-10_nice_rpetersen.pdf

[11]. Cybersecurity Framework | NIST. [Online]. Available: https://www.nist.gov/cyberframework.

[12]. National Centers of Academic Excellence. [Online]. Available: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/