K-12 Cybersecurity Education, Research, and Outreach

Giti Javidi
Information Technology
University of South Florida
Sarasota, FL
gjavidi@usf.edu

Ehsan Sheybani
Information Systems and Decision Science
University of South Florida
Sarasota, FL
sheybani@usf.edu

***Abstract* — This research-to-practice work-in-progress addresses a new approach to cybersecurity education. The cyber security skills shortage is reaching prevalent proportions. The consensus in the STEM community is that the problem begins at k-12 schools with too few students interested in STEM subjects. One way to ensure a larger pipeline in cybersecurity is to train more high school teachers to not only teach cybersecurity in their schools or integrate cybersecurity concepts in their classrooms but also to promote IT security as an attractive career path. The proposed research will result in developing a unique and novel curriculum and scalable program in the area of cybersecurity and a set of powerful tools for a fun learning experience in cybersecurity education. In this project, we are focusing on the potential to advance research agendas in cybersecurity and train the future generation with cybersecurity skills and answer fundamental research questions that still exist in the blended learning methodologies for cybersecurity education and assessment. Leadership and entrepreneurship skills are also added to the mix to prepare students for real-world problems. Delivery methods, timing, format, pacing and outcomes alignment will all be assessed to provide a baseline for future research and additional synergy and integration with existing cybersecurity programs to expand or leverage for new cybersecurity and STEM educational research. This is a new model for cybersecurity education, leadership, and entrepreneurship and there is a possibility of a significant leap towards a more advanced cybersecurity educational methodology using this model. The project will also provide a prototype for innovation coupled with character-building and ethical leadership.**

Keywords—Cybersecurity Education, Research, Outreach, K-12, Entrepreneurship, Leadership.

I. INTRODUCTION

Cybersecurity has originated from computer science (CS), but has emerged into a major concern in many other fields. Cybersecurity education and skills training is an unavoidable endeavor for all federal, state, and private organizations. In lieu of recent international cyber attacks, this effort has amounted to billions of dollars in financial damages and millions of human hours. The authors believe that such training should start in K-12, most likely incorporated in Advanced Placement (AP) CS courses. With this effort we will be able to build a diverse pipeline of students who would be interested in CS, cybersecurity, and other technology related fields. However, high schools are experiencing shortage of qualified teachers who can teach CS and cybersecurity. But also, we believe that cybersecurity concepts should be integrated in any curriculum. Therefore, all high school teachers must be aware of security issues and be equipped with resources to teach those concepts. To remedy this problem, our goal is two-fold: 1) to train teachers from all disciplines to teach cybersecurity concepts and 2) to revamp AP CS courses with an emphasis on cybersecurity.

Therefor, the goal of this project is to develop and validate a Cybersecurity curriculum as a model to help high school students develop an interest in cybersecurity, which is one of the fastest-growing careers. According to Cisco, there are more than 1 million jobs in the field of security that are unfilled [1]. To address this issue, federal, state, and private organizations are working together to raise awareness and increase the cybersecurity talent by providing training, workshops, and certifications. Many universities now offer cybersecurity undergraduate and graduate degrees, concentrations or certifications. Government agencies are also providing resources to colleges and universities in an effort to build a larger cybersecurity workforce. Florida Center for Cybersecurity (FC^2), at University of South Florida (USF), is a good example of this emerging approach, with an annual budget of $5 million.

The authors have already started building CS and cybersecurity foundation in Florida K12 school systems by exposing teachers to basic CS concepts

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

as the first step. The next step would be to continue with the instructions to introduce cybersecurity activities that can be used as stand alone or as part of the AP CS curriculum, depending on the teacher population. Cybersecurity is an interdisciplinary area. So, naturally, cross-disciplinary skills, such as the ability to find business solutions to social problems, are necessary to build an effective, efficient, and diverse workforce.

By training more high-quality teachers, the project will directly drive results for students. Our approach will not only improve teachers' and students' technological skills but also provide the means for engaging students with key local and societal crises to become global problem solvers. Through collaboration among multiple partners, this project will initiate an effort in the CS and cybersecurity education in high schools with the goal of developing aptitude and practical ability in young people to provide business solutions to social and global security problems.

II. UNIQUE NATURE OF CYBER SECURITY

Report from the Bureau of Labor and Statistics [2] shows that the demand for occupations in information security is growing at a rate of 28% by 2026, which is faster than average [2].

As the population of underrepresented minorities and females are not well represented in the cybersecurity professional realm. For example, data from Bureau of Labor Statistics [24] gives a clear picture of such underrepresentation in Information Security Analyst, as shown in Fig. 1.

Job	Total	Women	White	Black or African American	Asian	Latino
Info. security analysts	105	20.2	68.5	15.6	12.6	4.6

Fig 1. Labor force Statistics

Therefore, leveraging an emerging underrepresented minority and female group of high school students is an ideal strategy to consider. This will have the added benefit of utilizing a population that would add substantially to the number and diversity of professionals in the field. Therefore, it is the goal of this project to provide training to teachers who represent schools with the most diverse population of students.

One of the shortcomings in K-12 education is that students are taught to use various technologies, but they are not introduced to the threats they face while using them. Cybersecurity awareness, education and training as defined by National Institute of Standards and technology (NIST) [18] are all important components of our model. NIST [18] defines "awareness" as teaching students about security concerns and threads and teaching them to respond accordingly, "training" as teaching necessary security skills to tackle security issues, and "education" as combining all the skills to gain an understanding of the concepts and accumulate knowledge to respond to security issues. Simply put, education is anticipated to provide long-lasting foundational skills, while training provides specific skills as needed. Since both education and training are needed to fulfill the role described by our definition, this project provides activities applied to awareness, education and training.

As mentioned before, some of these issues stem from the lack of cybersecurity understanding of the teachers. Therefore, by training more high-quality teachers, the project will directly drive results for students.

While there are many proven strategies to increase participation and retention in CS, little has been done in the field of Cybersecurity [15]. There are some differences between the fields of cybersecurity, CS, and engineering education. In order to develop recruitment strategies, it is important to identify these differences because the many of the existing strategies in computer engineering (CE) and CS may not be applied to the Cybersecurity field [15]. Cybersecurity is a multi-disciplinary field which borrows information from CS, CE, Mathematics, Social Science, Business, and other disciplines [4]. However, it is an essential part of CS and should be integrated in CS curriculums to attract more students into the field.

III. SIGNIFICANCE

The cyber security skills shortage is reaching prevalent proportions. The consensus in the STEM community is that the problem begins at k-12 schools with too few students studying STEM

subjects. One way to ensure a broader pipeline in cybersecurity is to train more high school teachers to not only teach cybersecurity in their schools or integrate cybersecurity concepts in their classrooms but also to promote IT security as an attractive career path. The proposed research will result in developing a unique and novel curriculum and scalable program (leveraging cybersecurity certificate programs) in the area of cybersecurity and a set of compelling tools for a fun learning experience in cybersecurity education, leadership, and entrepreneurship. In this project, we are focusing on the potential to advance research agendas in cybersecurity and train the next generation of cybersecurity researchers and answer fundamental research questions that still exist in the blended learning methodologies for cybersecurity education and assessment.

The modules will be designed in format that they can be used as part of AP CS course or as standalone lesson plans that can be infused into social science, business, humanities, political science, psychology or any other courses where the topics fit. Students will also be supported by a virtual community of practice (COP) to provide a way for teachers, parents, students and other stakeholders to stay connected. The authors have already created a COP for Florida teachers to keep the connected with each other and the expert AP CS teachers in the area.

Leadership and entrepreneurship skills are also added to the mix to prepare participants for real-world problems. Delivery methods, timing, format, pacing and outcomes alignment will all be assessed to provide a baseline for future funded research and additional synergy and integration with existing, funded cybersecurity programs to expand or leverage for new cybersecurity and STEM educational research [5-7]. This is a new model for cybersecurity education, leadership, and entrepreneurship [8-10] and there is a possibility of a significant leap towards a more advanced cybersecurity educational methodology using this model. The model includes strategies for increasing cybersecurity pipeline by training teacher, parent and the community leaders alongside the students. Also, other stakeholders and industry experts have to be engaged in this effort as shown in Fig. 2.

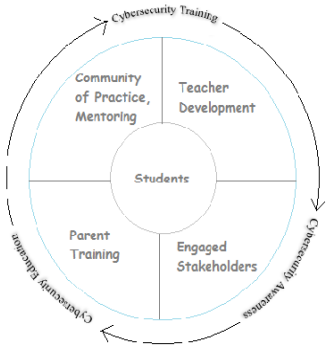

Fig 2. Increasing Cybersecurity Pipeline

K-12 cybersecurity education, research, and outreach is a much-needed area of information technology to keep up with future needs of science and engineering. The proposed research will further the researcher's scholarly achievements in a number of ways. The research topic is a unique idea in the field of cybersecurity. As such, attempting the research has the practical benefit of enabling the researcher to expand and disseminate the idea, improve teaching by presenting cutting-edge research and project ideas, find collaborators from across the world to advance the research, and plan future studies and funding sources.

IV. RELATED WORK

Due to the new nature of cybersecurity, there is not much research on cybersecurity education at k-12 level. Much of the research is in the areas of computer science and technology education. Therefore, there is need for more research in this area at the k-12 level.

The subject of gamification [19] [21] [22] seems to be getting much attention in the cybersecurity training and education. Researchers at Purdue University Northwest [19] used a game-based approach to teach cyber security to 154 high school students. The topics included “social engineering and information security concept, secure online behaviors and cybersecurity first principles [19]”. The results indicated that the male participants enjoyed the activities more than female participants [19].

At undergraduate level, researchers have also attempted to infuse criminal justice and political

science concepts into cyber security courses to give a deeper understanding of cyber threats [20].

Payne and Abegaz [23] report "a modified scrum framework (GenCyberScrum) for the NSA-NSF GenCyber program introducing high school students to ten cybersecurity first principles". Students developed physical and virtual representations of all ten cybersecurity first principles through "3D printing, 3D animations in Alice, Sketches/Gestures, Fuzzy Stick Models, and Sphero robotic light drawings [23]".

V. Theoretical Foundation

Cybersecurity training requires teams of experts from various disciplines with different knowledge, expertise, and perspectives, which will include computer scientists, forensic scientists, and business and social entrepreneurs. In order for the new generation to be cyber aware, they must have a good foundation in cyber threads and risks. Therefore, due to multidisciplinary nature of cybersecurity, we are proposing an integrated curriculum based on Leonard's Integrative Learning Theory [16]. According to Adria Steinberg [17], creating a successful project-based multidisciplinary integrated curriculum includes six basic principles [17]:

1. Academic and technical rigor
2. Authenticity
3. Applied learning
4. Active exploration
5. Adult connections
6. Assessment practices

We are hoping that this integrative curriculum and associated lesson plans and units can help high school teachers to reinforce cybersecurity concepts in their classrooms.

VI. Participants and Methods

The primary goal of this pilot project is to establish a Cybersecurity Pipeline in the Sarasota-Manatee school districts to increase the supply of qualified high school teachers to help raise interest in high school students to pursue cybersecurity as one of the STEM-related careers. The project will target 10 high school teachers in several Florida School Districts (FSD), Manatee and Sarasota, and will provide them with experiences with emerging technologies in cybersecurity. K-12 teachers play an instrumental role in preparing the STEM pipeline. The project intends to expose the teachers to deeper learning for engagement that seeks to harness technology, through stimulating inner creativity and critical thinking in cybersecurity. All participants will receive a minimum of 40 hours of hands-on summer training. Participants will be trained to integrate cybersecurity technology into their curriculum, serve as advisors to students, and aid in developing strategies for fun-learning activities (e.g. Maker-Space, Hackathon, and Shark Tank). They will also learn strategies to encourage students to imagine business-based solutions to social problems using technology. As a result, students will enhance tech skills, discover new career directions, and build their online brand. Their network will be enriched by partnerships with industry and tech leaders. The ultimate goals are to expose high school teachers (and as a result, students) to careers in cybersecurity field, establish tech innovator model for entrepreneurial thinking, deliver an online resource to disseminate curriculum, and promote an enriched ecosystem model for cybersecurity learning in high schools.

VII. Project Status And Trajectory

The authors have experience and expertise in recruitment, retention, education, training, and outreach to underrepresented minorities and females. The authors have a long list of publications and federal and private funded projects pertaining to the same. These speak to authors' experiences with teacher training [11], minority recruitment and retention [12], teaching strategies [13], and STEM education and training [14]. The authors have already established a strong tie with Florida School Districts and area teachers through other projects. They are in the process of developing summer course plan and curriculum based on the proposed plan and testing the validity of the approach. In a parallel and separate research project, they will develop tools to generate assessment rubrics for measuring the effectiveness of the project. The first project will take place during July 2018, followed by the second project that will continue until November 2018.

REFERENCES

[1] Cisco Report, "Mitigating the cybersecurity skills shortage: Top insights and actions from Cisco security advissory services", Cisco, 2015. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf [Accessed: May 12, 2018].

[2] Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, Information Security Analysts. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm [Accessed: June 07, 2018].

[3] Whitehouse Report on Forign Policy, "The Comprehensive National Cybersecurity Initiative", Whitehouse. [Online]. Available: https://obamawhitehouse.archives.gov/node/233086 [Accessed: May 12, 2018].

[4] M. Darke, (2002). Defining a Curriculum Framework in Information Assurance and Security, Cerias Technical Report, 2002-68, Cerias, Purdue University, 2002.

[5] R. Bell and H. Bell, (2016). "Replicating the networking, mentoring and venture creation benefits of entrepreneurship centres on a shoestring: A student-centred approach to entrepreneurship education and venture creation". *Industry and Higher Education*, 30(5), 334-343.

[6] B. Hynes, N. Kennedy, J. Pettigrew, (2016). "The Role of Business Schools in Framing Entrepreneurial Thinking Across Disciplines: The Case of Allied Health Professions". *In Innovative Business Education Design for 21st Century Learning*, Springer International Publishing, pp. 75-91.

[7] C. Mason, (2011). "Entrepreneurship education and research: emerging trends and concerns". *Journal of Global Entrepreneurship*, 1(1), 13-25.

[8] S. L. Nielsen and W. B. Gartner, (2017). "Am I a student and/or entrepreneur? Multiple identities in student entrepreneurship", *Education + Training*, 59(2), pp.135-154.

[9] R. Nyello, N. Kalufya, C. Rengua, M. J. Nsolezi, and C. Ngirwa, (2015). "Effect of Entrepreneurship Education on the Entrepreneurial Behaviour: The Case of Graduates in the Higher Learning Institutions in Tanzania". *Asian Journal of Business Management*, 7(2), 37-42.

[10] Z. Zeng and B. Honig, (2016), "How Should Entrepreneurship Be Taught to Students with Diverse Experience? A Set of Conceptual Models of Entrepreneurship Education", in Jerome A. Katz , Andrew C. Corbett (ed.) *Models of Start-up Thinking and Action: Theoretical, Empirical and Pedagogical Approaches (Advances in Entrepreneurship, Firm Emergence and Growth,)* Volume 18, Emerald Group Publishing Limited, pp.237 - 282

[11] G. Javidi and E. Sheybani, "Empowering Teachers to Raise Career Awareness in Computing: Lessons Learned", *Journal of Systemics, Cybernetics and Informatics (JSCI)*, Vol. 15, No. 3, pp. 10-15, 2017.

[12] G. Javidi and E. Sheybani, "An Understanding of factors influencing retention of African-American undergraduate students in computer science", *Journal of Innovation in Education (JIE)*, Vol. 4, No. 1, pp. 66-77, 2017.

[13] G. Javidi and E. Sheybani, "Teaching Computer Programming through Game Design: A Game-First Approach", *GSTF Journal on Computing (JoC),* Vol. 4, No. 1, 2014.

[14] G. Javidi, E. Sheybani, M. Talaiver, **"**Improving students' skills, knowledge and abilities in computer programming: a stem project", *Journal of Computing Science in Colleges*, Vol. 29, Issue 2, December 2013.

[15] R. Shumba, L. Hall, K. Ferguson-Boucher, Elizabeth Sweedyk et al. "Cybersecurity, women and minorities", In proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports - ITiCSE -WGR '13, 2013.

[16] J. B. Leonard, "Integrative Learning: A Grounded Theory", *Issues in Integrative Studies*, No. 30, pp. 48-74, 2012.

[17] A. Steinberg, *Real Learning, Real Work*. New York: Routledge, 1997.

[18] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program", *National Institute for standards and Technology, Computer Security Division,* 2003. [Online]. Available: http://www.iwar.org.uk/comsec/resources/security-awareness/sp800-50.pdf [Accessed: June 7, 2018]

[19] G. Jin, M. Tu, T. Kim, J. Haffron, and J. White, R. Jones, and K. Trello, "Adaptive filtering in data communications with self improved error reference," In Proceeding of the 49th ACM Technical Symposium on Computer Science Education, SIGCSE'18, 2018, pp. 68-73.

[20] M. Stockman, "Infusing Social Science into Cybersecurity Education", Proceedings of the 14th annual ACM SIGITE conference on Information technology education, SIGITE'13, 2013, pp. 121-124.

[21] K. Leune and S. J. Oetrilli, Jr., "Using Capture-the-Flag to Enhance the Eectiveness of Cybersecurity Education", In Proceedings of the 18th annual ACM SIGITE conference on Information technology education, SIGITE'17, 2017, pp. 47-52.

[22] C. Herr and D. Allen, "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors", In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, SIGMIS-CPR '15, 2015, pp. 23-29.

[23] B. Payne and T. Abegaz, "Gencyberscrum: improving cybersecurity education outcomes with the scrum framework", *Journal of Computing Sciences in Colleges,* V. 33, Issue 4, , pp. 60-68, 2018

[24] Bureau of Labor Statistics, Labor Force Statistics from the Current Population [online]. Available: https://www.bls.gov/cps/cpsaat11.htm [Assessed; June, 10, 2018]