Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students

Laurin Buchanan, Lori Scarlatos, Nataliia Telendii
laurin.buchanan@securedecisions.com, lori.scarlatos@stonybrook.edu, nataliia.telendii@stonybrook.edu

***Abstract* - To both broaden and increase participation in any STEM field such as cybersecurity, we need to attract more students. Research shows that to do this, students need to be engaged with cybersecurity during middle school. There is a lack of age-appropriate and classroom-ready cybersecurity curriculum, however, and many teachers feel unprepared to teach the subject. To address this gap, the CyberMiSTS project team created a summer professional development workshop for middle school teachers that integrated a recent research-based understanding of cybersecurity into a curriculum that is accessible to both middle school students and their teachers. The project sought to encourage participation of a broad and diverse set of students in the field of cybersecurity by showing them how human relations play an important role in cybersecurity. We discuss our prior related work using branching web comics to introduce middle school students to cybersecurity concepts and careers, and the state of evidence-based research into effective approaches and methods for cybersecurity education. We identify challenges to broadening the pipeline for a truly diverse cybersecurity workforce that can meet industry's need for cybersecurity professionals with a wide range of experience and skills. The paper introduces our approach for the teacher professional development workshop, maps how we designed the project to meet our research goals, and documents initial findings regarding what is needed to increase teacher self-efficacy about cybersecurity concepts and careers in a middle school classroom.**

Index Terms – cybersecurity education, K12, teacher professional development, careers

INTRODUCTION

The December 2020 Solar Winds Orion hack [1] that impacted both Fortune 500 companies and multiple agencies in the US government is a clear reminder that having an educated cybersecurity workforce is critical to both our national security and economic prosperity. The U.S. Bureau of Labor Statistics forecasts 31% job growth for information security analysts from 2019 to 2029 [2]. A recent Burning Glass report indicates that demand for cybersecurity workers in the United States has nearly doubled since 2013 and is growing three times as fast as other IT roles [3].

To grow the pipeline of future cybersecurity workers at a scale that can meet this continued and critical demand, we need to attract both more and more diverse students to cybersecurity. Cybersecurity is a multidisciplinary field that is in need of practitioners who understand the human in the loop: cybersecurity is a human problem, not a technology issue. The National Initiative for Cybersecurity Education (NICE) Strategic Plan vision is "Prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes America's national security and economic prosperity." As part of the NICE effort, the K12 Cybersecurity Education Implementation Plan was created to help create a coordinated, coherent set of national K12 cybersecurity education activities. The second item in this Implementation Plan is "Infuse Cybersecurity across the Education Portfolio" [4]. But how can teachers and schools achieve this?

There has been little evidence-based research showing what works in cybersecurity education, particularly in a K12 environment. Cybersecurity education in K12 has often focused on high school computer science classes and Career Technical Education (CTE) programs. Some recent research indicates, however, that to broaden participation in STEM, students in late elementary and middle school should be introduced to various careers that can improve health and safety [5] which may help them make personal connections to technology and related careers.

The Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students (CyberMiSTS) project was designed to research and identify what works in professional development for middle school teachers of cybersecurity, and what classroom approaches may succeed in engaging the interest of middle school students in the field of cybersecurity. We seek potential ways to successfully infuse cybersecurity across the middle school experience in order to expose all middle school students to cybersecurity concepts and careers, not just those in a computer science class. To make both the professional development and the resulting classroom curriculum broadly accessible for any teacher in any school, we planned a workshop with a curriculum that does not require computer labs or software installs. The ultimate goal is to identify methods and approaches that enable teachers of all subjects to develop their own introductory cybersecurity curriculum that is relevant to their students and reflects their cultural norms such as socioeconomic status, language, and access to

technology. This customized curriculum can support teaching in meaningful and authentic ways that are relevant to students' everyday lives, the antithesis of a "one size fits all" approach. Finding ways to make cybersecurity relevant to all students is essential to encouraging broader participation in the field.

PRIOR WORK

Comics are popular with people of all ages, and the use of words and pictures has been shown to scaffold learning [6], making them an increasingly popular educational medium in any classroom or field. For example, the use of comics in healthcare, called Graphic Medicine, can help both patients and medical professionals understand the human aspect of disease and treatment. The use of and scholarship on Graphic Medicine has rapidly accelerated since 2017 [7].

Branching web comics, where readers make choices on behalf of a character and see the consequences of those choices in the next scene, are a novel, interactive approach to teaching and assessing understanding. Branching web comics are a good approach for teaching cybersecurity because these stories give a learner the opportunity to make decisions and, more importantly, explore the consequences of those decisions in a safe environment.

Comic-BEE is a cybersecurity education technology developed by Secure Decisions and designed to facilitate the rapid creation of branching web comics for educational use. It was developed with funding from the U.S. Department of Homeland Security (Contracts HSHQDC-14-C-B0019 and HHSP233201600057C) as a way to create competitions and challenges that would attract less technical learners of all ages to cybersecurity, as an alternative to the more technically demanding Capture the Flag cybersecurity competitions that challenge participants to solve computer security problems and/or capture and defend computer systems. The Comic-BEE effort built on a small research program for the Air Force [8] which used branching comics to provide safe computing training for airmen and office workers. The Comic-BEE web application provides an integrated, guided process for educators and subject matter experts to plan the lesson for their comic, write the script of their branching story showing positive and negative outcomes, rapidly storyboard the essential visual layout of their comic scene by scene, and format the comic with full color artwork prior to online delivery and presentation [9].

In our team's prior Branching Interactive Graphic Stories for Cybersecurity Education (BIGSCE) project, sponsored by the National Science Foundation (Awards DGE-1623150, DGE-1623131), we used design research methods to refine an approach to teaching middle school kids about cybersecurity by having them read, reflect on, and then write their own comics about cybersecurity using Comic-BEE. In the 10-day BISCE workshops, students read a comic about cyber ethics that was set in a middle school, and another comic that detailed a real-world forensic investigation. Students made choices on behalf of characters which caused their comic story to follow a variety of branches with different outcomes, some good and some bad. We led the students through discussions of story choices and outcomes, cybersecurity careers and myths and misconceptions about cybersecurity concepts and careers. We modeled with the students three types of questions that could help identify malicious activity: *Has any unusual network activity been observed? Have we seen anything like this before? Are there known weaknesses (vulnerabilities) in the computer systems or networks?* Students were then given a scenario involving pirates using cyber weaknesses to attack container ships and steal valuable cargo (again, based on actual events) and worked in pairs to create comics showing how a cyber crime investigator could use one of the three above questions to find out what had happened. Students also identify what cybersecurity work roles could help answer that question.

We gained valuable experience learning how to engage middle school students on cybersecurity, as well as how to use Comic-BEE to introduce different roles and career options in cybersecurity to the students. Recruiting students to the afterschool program was a challenge, however: teachers and administrators recommended the program to their best and brightest math and science students, despite information that no prior cybersecurity or computer science experience was needed for the program. The lessons learned from BIGSCE led us to conclude that in order to make a real impact and really reaching a broader group of students, we needed to change our focus to classroom teachers. The BIGSCE experience also had significant influence on both the approach and content of the CyberMiSTS professional development workshops.

I. Diversity in Cybersecurity

Diversity in the workplace generally is believed to foster creativity, drive innovation, and increase productivity and performance [10]. A recent report indicated that women now comprise 24% of the cybersecurity workforce; this was in large part due to a broader definition of cybersecurity work roles [11]. However, real diversity in cybersecurity should include more than just demographics. Cybersecurity is a multi-disciplinary field with legal and ethical impacts across every business sector. Practitioners working to create, design, test, and implement solutions, and educate others need to understand the humans in the loop. Cybersecurity practitioners who have different expertise and perspectives, including social sciences like economics, psychology, human factors and cognition, are just as necessary as practitioners with different areas of technical expertise.

[12] presents a systematic review of various educational efforts to broaden participation and diversify the cybersecurity field, seeking to identify the current body of work, gaps in research and approaches that are successful or unsuccessful. Among the gaps noted is the lack of any substantive and systematic evaluation of interventions, including their effect. This true for both college interventions as well as camps and other pre-college activities. One recommendation is to include education researchers in these efforts as a way to improve engagement opportunities with

underrepresented groups, rather than relying solely on technical researchers and practitioners. Another is to infuse cybersecurity across the post-secondary landscape by using concepts such as ethical privacy issues or social engineering to create general education interventions that demonstrate the multidisciplinary aspects of cybersecurity.

As discovered by Ladson-Billings, who developed the theory of *culturally relevant pedagogy*, diverse groups of students are more academically successful when their differences are appreciated and celebrated, and those differences are brought to bear in the real world. In particular, she emphasizes the importance of encouraging students "to consider critical perspectives on policies and practices that may have direct impact on their lives and communities" [13]. Cybersecurity is an important socio-scientific topic with great potential for showing cultural relevance. Getting students to understand the impact that cybersecurity has on their own lives is one way of doing this.

II. Cybersecurity in K12 Education

A key finding in a recent government report stated, "There is an apparent shortage of knowledgeable and skilled cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors" [14]. This gap for K12 was first noted in a 2010 educator survey that indicated cybersecurity preparation and training for K12 teacher was scarce [15]. A lack of access to technology and curriculum was also noted at that time. A more recent but similar national survey on the state of K12 cybersecurity education indicates only 45% of educators surveyed indicate their students are learning about cybersecurity [16]. This latest survey also points out the substantive equity issues that exist: students at public schools, or in small or high poverty districts, or where cybersecurity is not offered at local universities, or where cybersecurity companies are not part of the local industry, are likely to have less access to cybersecurity curricula. The survey also indicated that most educators reported that cybersecurity curriculum is "infused across curriculum," rather than conveyed in a stand-alone cybersecurity course, but did not provide any indication of how this has been implemented or any description of the curriculum content.

Teachers often still have insufficient preparation to teach the still new subject of cybersecurity, and they lack a curriculum that is ready for their classroom. The National Initiative for Cybersecurity Careers and Studies Education and Training Catalog (https://niccs.cisa.gov/training/search) exists for cybersecurity professionals, however, there is currently no equivalent content repository for K12 learners or educators that can direct them to accurate and effective cybersecurity curricular content and materials. The CLARK repository of curriculum at https://clark.center is intended for post-secondary education, it does not have curricular materials for middle school students. Members of the NICE K12 Community of Interest (NICEK12) recently created "NICE @ Home" (https://nicek12athome.weebly.com), a curated list of online resources for students, parents, and educators to promote cybersecurity content, particularly during the COVID-10 pandemic. NICEK12 is leading a "Content Review and Repository Recommendations" project[1] which is collecting and reviewing K12 educational materials using an evaluation rubric based on the Change the Equation STEM evaluation rubric [17]. The ultimate goal of the project is to provide a searchable, online repository of curricular materials that teachers can trust.

As our own research projects have indicated, there are both middle and high schools that still do not have computer science classes or labs. There are districts where teachers do not receive regular and updated cybersecurity awareness training, and as a result are often uncertain about basic cybersecurity principles. Conferences like the annual NICE K12 Cybersecurity Conference (https://www.k12cybersecurityconference.org/) provide opportunities to share overviews and lessons learned with other attendees, however, without conference proceedings, very little actionable information about successful efforts is subsequently published or even widely disseminated.

As seen in [12], much of the published research in K12 cybersecurity education has focused on CTE and high school curriculum, and therefore is received primarily by students who are already interested in computers and/or cybersecurity, rather than attracting different thinkers to the subject. Computer science education frameworks, such as the K12 Computer Science Framework (https://k12cs.org/) may include statements about cybersecurity, but they do not provide curriculum or assessment content. TeachCyber.org is an ongoing effort to adapt curriculum guidelines [18] into a one-year module for high school students planning to enroll in cybersecurity college program. Cyber.org offers a range of K12 STEM curriculum that incorporates cyber literacy and a cyber science course, but it has not previously included assessments, which can be a barrier for classroom use in many schools. Professional development for teachers aligned with this curriculum content is available online and in person through Cyber.org.

The GenCyber program (https://www.gen-cyber.org) provides funding for a limited number of cybersecurity education camps for high school students, as well as professional development camps for K12 teachers. The individual camps are run by universities with cybersecurity programs, so access is further restricted to teachers who either live locally or are able to travel for a week. Each camp develops its own curriculum and activities based on local expertise. Given the competitive nature of the program funding, participating institutions are actually incentivized to not publicly disseminate either their curriculum or outcomes.

Created as part of an undergraduate degree program, the National K-12 Cyber Security Education Project Directory (https://www.cyberroots.org) is a searchable repository of programs that focus on cybersecurity educational opportunities for K12 students, including educator training programs. It is unclear at this time if the project will be

[1]https://www.nist.gov/document/nicek12subgroupprojectcharterconten trepository-2pdf

actively maintained in the future.

Cybersecurity is not the only new technology field to which students need to be exposed. The rapid advances in artificial intelligence and other evolving technologies will result in new job opportunities by 2030. There is a clear need for research to identify what has worked for rapid and effective teacher preparation and classroom approaches in other subjects so those those lessons learned can be applied to K12 cybersecurity education. In turn, cybersecurity educators and researchers need to seek evidence of what is and is not successful in their own efforts, and disseminate those findings widely and rapidly.

CyberMiSTS Approach

The CyberMiSTS project has three aims. First, integrate recent research-based understanding of cybersecurity into a middle school curriculum that motivates students and improves learning outcomes. Second, identify what teachers need to be successful with teaching cyber in a middle school classroom and, based on this, develop curricula and resources for disseminating this teacher instruction nation-wide. Third, encourage participation of a broad and diverse set of students in the field of cybersecurity by showing them how human relations play an important role in cybersecurity.

To meet these aims, we created a professional development workshop for teachers. Initially this workshop was designed for middle school Career and Technology Education (CTE) teachers. However, we have found that this workshop is suitable for any middle or high school teacher who wishes to teach a unit on cybersecurity. We also initially designed the workshop for a face-to-face setting, but had to run it synchronously online in the second year of the project due to the global pandemic. Fortunately, we found that both modes work equally well.

The workshop consists of approximately 60 contact hours that include lectures, hands-on activities, guided research, and the development of a customized curriculum that includes an instructive branching comic targeted at the teachers' audience. Figure 1 shows how these components build on one another. We wanted to give each participant the opportunity and the resources to develop their own plan for teaching their own students about cybersecurity. We remind participants of this objective throughout the workshop, starting on the first day, so that teachers do not lose sight of why they are there and ensure they to reach this goal.

Although we want workshop participants to understand some very technical concepts, it would be unrealistic to expect teachers (with limited or no background in the subject) to become cybersecurity experts in such a short period of time. We therefore chose to focus on topics that are of greatest importance to the students, at a level that all teachers could reasonably master. The topics we chose to cover were Data Protection, Web Security and Privacy, and Cybersecurity Careers. The Data Protection topic covered threats, vulnerabilities, and attacks; protections against threats (confidentiality, integrity, availability, authentication, authorization, privacy and anonymity); the various states of data (in use, in transit, and at rest); malware and defenses against it; and defense against threats to data in the various states. The Web Security and Privacy topic covered securing data on the internet; secure password creation; hashing; authentication; phishing and how to identify a potentially problematic domain; network protocols and maintaining integrity and confidentiality; and web tracking. The Cybersecurity Careers lectures covered categories of cybersecurity jobs; education and skills required to attain various positions; and cybersecurity career paths. All three subjects were taught by cybersecurity experts.

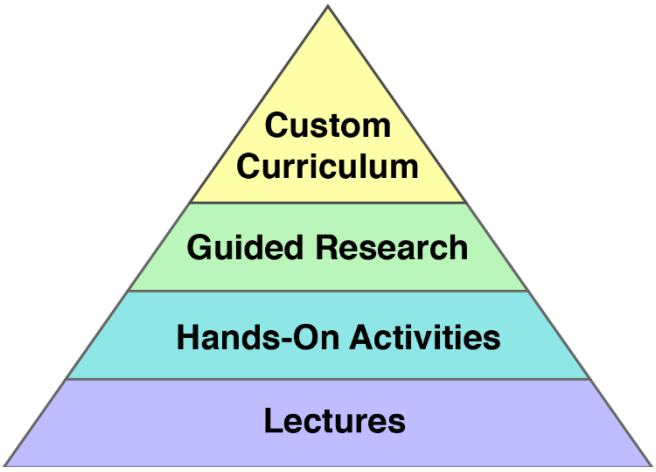

FIGURE I
WORKSHOP COMPONENTS

Hands-on activities give participants the opportunity to put what they've learned into practice. For example, after discussing how attackers use compromised passwords for credential stuffing attacks at different websites, participants were directed to the Have I Been Pwned? website (https://haveibeenpwned.com/). There they discovered if any of their email accounts had already been reported compromised as part of a known website breach. All activities need to be followed with a group discussion of the experience to further cement their understanding of the lessons; in this case, there was a long discussion regarding how participants could secure their accounts.

Guided research activities give participants the opportunity to find out more about what they have just learned. For example, early in the workshop, participants were asked to find recent news articles about a data breach. Our guidance includes asking the participants to think about what their own students would find interesting and/or compelling, and how they could work that into their lessons. Participants are placed into small groups so that they can develop a strategy for doing the research, discuss their findings after working independently, and then decide how to report back to everyone.

A major portion of the workshop is devoted to the development of an instructive, branching comic. Created with Comic-BEE (https://comic-bee.com), the comic is designed to get students to think about choices and consequences within the realm of cybersecurity. Comics are developed in

four phases. In the first phase, the author develops a lesson plan for the comic, explicitly delineating the concepts covered, the skills/knowledge/understanding (SKU) that students are expected to derive, and specific learning objectives related to the SKUs. Careful planning in this phase helps to ensure that the comic will be an important part of the learning experience for students reading the comic. In the second phase, the author defines scenes (which will ultimately translate to screens) in the story and choices that will determine what happens next. The author then uses choices to link scenes together, creating the flow of the story, from a common beginning to one of several possible endings, depending on the choices made by the reader. Figure 2 shows a screenshot of this phase in Comic-BEE and how choices are associated with learning objectives, ensuring alignment with the lesson plan. In storyboarding, the third phase, the author translates this story to a visual format. Visuals in this phase are reduced to simple outlines and stick figures with their dialog, enabling the author to quickly make changes in presentation. In the final phase, the author replaces those simple outlines with selections from a rich library of SVG graphics with a diverse set of potential characters. The Comic-BEE website provides extra help, videos, frequently asked questions, and blogs focused on the best approaches to take when creating comics. We also created a demonstration comic that participants could upload and manipulate while learning the Comic-BEE application.

As participants develop their comics, they are also asked to think about their overall plan for teaching cybersecurity to their students. They are given a lesson plan template in which they indicate concepts being taught, expected learning objectives, supplemental activities, and assessments they will use in the classroom. We give them sample assessments that they are free to modify and use as they deem appropriate.

Because teachers are expected to deliver their curricula to the classroom, they are brought back for a follow-up symposium after they have taught their lessons to students. In this symposium, the teachers share their experiences and lessons learned. They also share anonymous data from their students demonstrating the impact of their lessons.

To help ensure that all of this was helping to achieve the aims of the project, we developed a research plan that delineates research questions, related hypotheses, and a set of data to be collected and analyzed. The research questions are based on the three aims of the project. Toward the first aim, we ask two questions: Q1) Self-efficacy: *to what degree do participants feel confident that they can teach their students about cybersecurity?* Q2) Learning: *to what degree do*

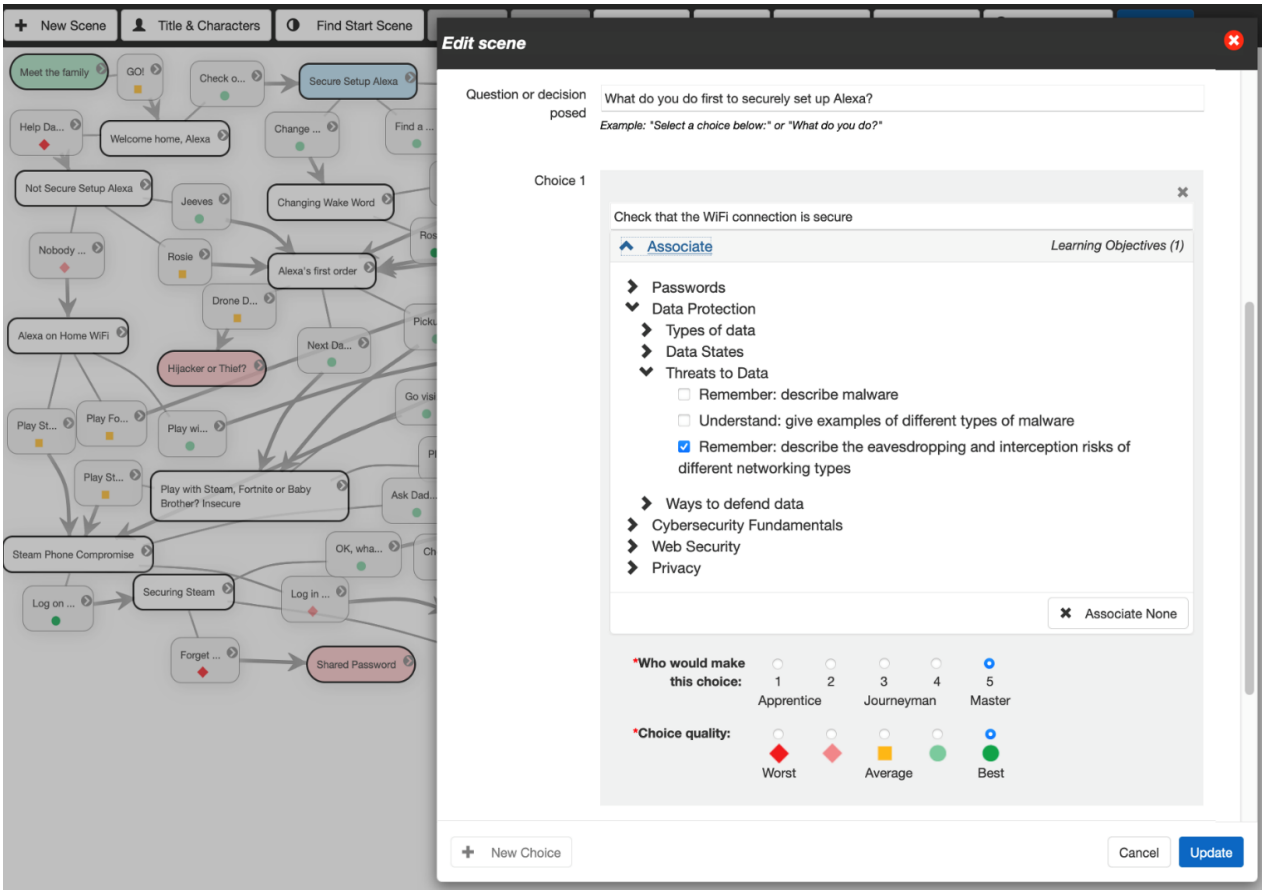

FIGURE 2

USING COMIC-BEE TO EDIT A SCENE IN A BRANCHING SCRIPT, ADDING CHOICES WHICH LEAD TO SUBSEQUENT SCENES AND ASSOCIATING CHOICES WITH LEARNING OBJECTIVES FROM THE COMIC'S LESSON PLAN

participants' actual understanding of cybersecurity change over the course of the workshop? Toward the second aim, we ask two questions: Q3) Satisfaction: *how do participants feel about the workshop and their own abilities, and how does that change over time?* Q4) Preparation: *how prepared are teachers, at the conclusion of the workshop, to teach their students about cybersecurity*? Toward the third aim, we ask one question: Q5) Student outcomes: *what is the impact on students when these lessons are brought to the classroom*? Data were collected during the workshops and the symposium. Table 1 shows what was collected, the time when it was collected, and the questions they are meant to answer. Under Time, codes represent daily (D), the beginning of the workshop (B), the start of learning a new topic (Ts), the end of the learning period for a topic (Te), the conclusion of the workshop (C), and the follow-up half-day symposium (S). Our findings are described in the next section.

TABLE I
DATA COLLECTED

Time	Data collected	Q1	Q2	Q3	Q4	Q5
B, C, S	Self-efficacy survey	X		X		
Ts, C	Free-listing activity		X			
Te	Content quiz		X			
D	Daily satisfaction survey			X		
D	Journey map	X		X		X
C	Teacher's comic				X	
C	Teacher's curriculum plan				X	
B, C	Scored comic		X			
D	Videotaped roundtable discussions			X	X	
S	Anonymized student data				X	X

RESULTS

Two workshops were offered: one face-to-face over 2 weeks (6 hours per day) in the summer of 2019 and the other online using Zoom over 3 weeks (4 hours per day) in the summer of 2020. A total of 18 teachers signed up for the workshops; 14 of them completed a workshop. Only one symposium for sharing student outcomes has been held to date; 4 teachers participated in that. Due to space constraints, we are only summarizing our results here. A more detailed report of the results is being developed for a subsequent journal paper.

Self-efficacy: To measure teachers' initial knowledge and confidence to teach cybersecurity concepts and capture the impact of the workshop on participant teachers, we developed a survey on cybersecurity self-efficacy and readiness to teach cybersecurity concepts. For these surveys we drew heavily on an early published report on cybersecurity preparedness of preservice teachers [19], the 2012 report from the National Cyber Security Alliance [20], and a report on cybersecurity education for community college faculty [21]. Participants' confidence in their ability to teach the information learned in the workshop generally increased. Figure 3 shows the change in teachers' confidence in their ability to teach cybersecurity fundamentals.

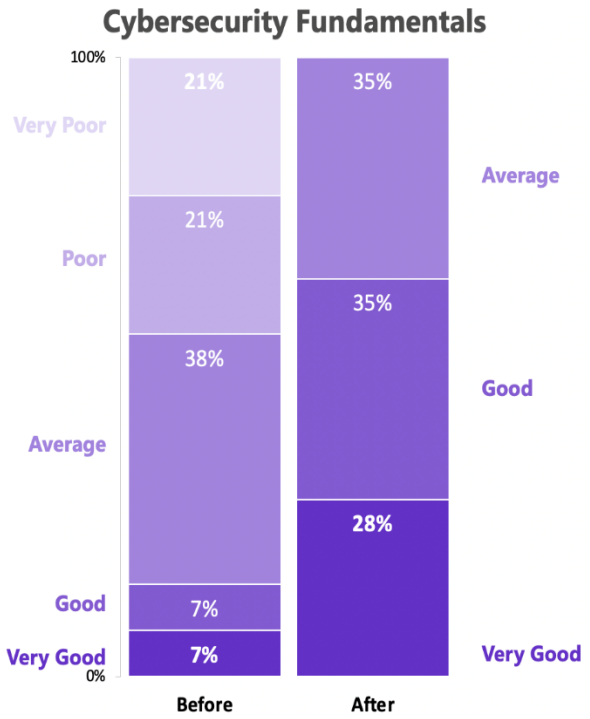

FIGURE 3
CHANGE IN TEACHERS' CONFIDENCE IN THEIR ABILITY TO TEACH CYBERSECURITY FUNDAMENTALS TO THEIR STUDENTS

Learning: As might be expected, participants learned and came to understand new terminology and concepts. We used two measures to determine this. First, we used a free-listing activity to determine participants' free associations with cyber-centered terminology, words such as compromise, vulnerability, and malware. This was done before and after participants learned a new concept, to show the change in their understanding. Results show that in many cases, participants came to understand the terms' relation to cybersecurity. Second, we gave participants a quiz at the end of each learning unit to gauge their understanding of what was learned. These questions were derived from the assessment materials created by the Catalyzing Computing and Cybersecurity in Community Colleges (C5) project (https://www.ncyte.net/about-c5) funded by the National Science Foundation. Third, we looked at the concepts covered in the teacher comics, which were inspired by the lessons in the workshop.

Satisfaction: Participants' satisfaction with the workshop, and with their own progress, was lowest at the beginning of the workshop. This was especially true for participants who had misconceptions regarding the goals of the workshop. All participants struggle with the new material initially; as they hear the same terminology used over and over in various contexts, they become more comfortable, confident, and knowledgeable.

Preparation: The workshop does appear to prepare

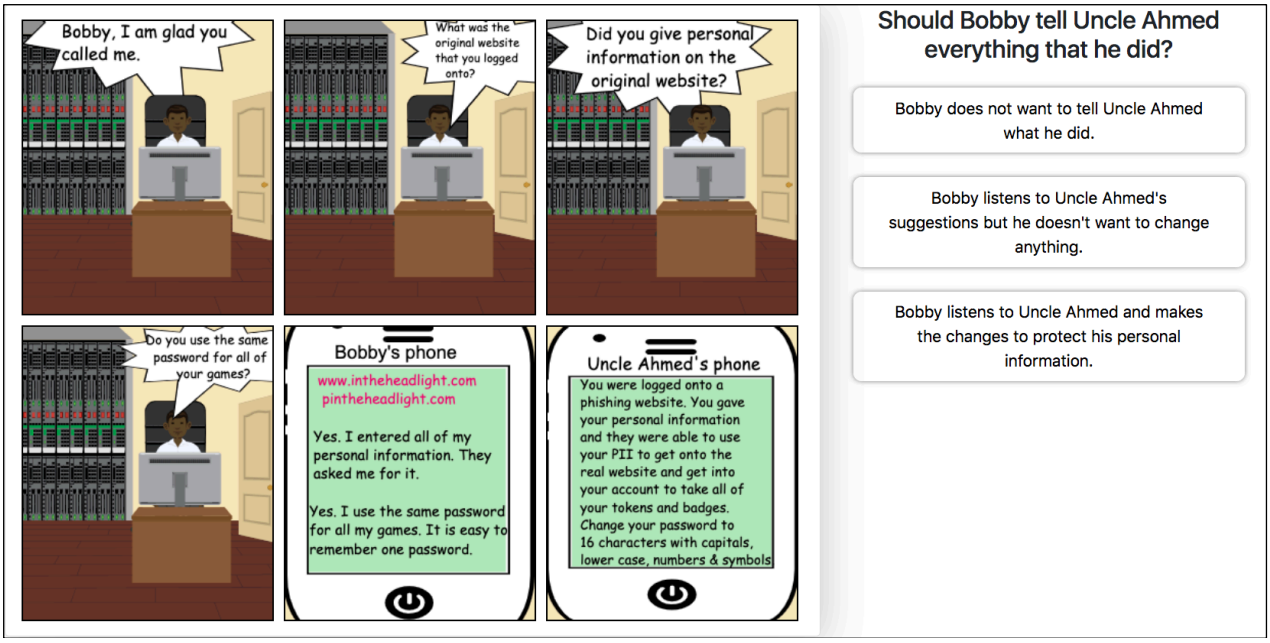

FIGURE 4
SCENE FROM A PARTICIPANT'S COMIC ON PERSONALLY IDENTIFYING INFORMATION

teachers to teach cybersecurity in their classrooms. Their lesson plans are well thought out, and their instructive comics are engaging, as seen in the example in Figure 4. Teachers who delivered their lessons in the classroom and then participated in the symposium also shared stories and lessons learned which indicated that they felt that they were successful in teaching cybersecurity to their students.

Student outcomes: The student data -- which includes test results, videos, comics, and reflections -- shows that the students did learn some things about cybersecurity concepts and careers. Some of them even expressed interest in further exploring cybersecurity careers.

CONCLUSIONS

Data collection and analysis are ongoing; we will hold our second symposium this summer, where teachers from both workshops will be given an opportunity to report on their experiences teaching cybersecurity. Yet, with this work we have gained some important insights regarding professional development for teachers learning a new technical subject.

- Participants need to have a clear understanding of the goals of the professional development and what will be expected of them. We found that better-informed participants were less likely to drop out before the workshop concluded.
- Teachers need a rich set of resources available to choose from, to help them bring the lessons back to the classroom. They also need ample opportunity to play with those resources to determine how appropriate they are for the teachers' students.
- Technical experts need to be involved in the delivery as well as the creation of the content. Participants often have questions regarding the content that were not anticipated ahead of time, and prompt and accurate answers need to be given in answer.
- When asked to teach new STEM topics, teachers struggle to find time to cover the material adequately. Teaching online can make this especially challenging.

Much work remains to be done. As we continue our analysis of the data, we are developing a model for the professional development of teachers learning a new technical subject. This should enable even more teachers to meet the growing demands of STEM education in our schools. We are also working on a paper focused on commonly held misconceptions about cybersecurity careers, and how we can attract more middle school students to the field. In the end, we need more people conducting case studies in differing regions, teaching cybersecurity at the middle school level and sharing their results. Only then will we gain a more complete picture of best practices for teaching cybersecurity to middle school students.

ACKNOWLEDGMENT

We would like to thank Drs Nicholas Nikiforakis and Michalis Polychronakis, members of the National Security Institute at Stony Brook University, who taught the workshop content on data protection and web security and privacy. We also thank the members of our advisory board who provided important insights and suggestions: Dr. Susan Lowes, Ms. Darlene Roces and Ms. Heather Ciccone. This work was supported by a grant (awards #1821753 and #1821757) from the National Science Foundation.

REFERENCES

[1] Krebs, Brian (2020, December 14). U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise. [Blog post]. https://krebsonsecurity.com/2020/12/u-s-treasury-commerce-depts-hacked-through-solarwinds-compromise/. Accessed January 4, 2021.

[2] Bureau of Labor Statistics, U.S. Department of Labor. "Occupational Outlook Handbook, Information Security Analysts." https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. Accessed January 14, 2021.

[3] Markow, W., Bittle, S., and Liu, P. C. (2019). "Recruiting watchers for the virtual walls: the state of cybersecurity hiring." https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf.

[4] National Initiative for Cybersecurity Education (NICE) Community Coordinating Council. "National K12 Cybersecurity Education Implementation Plan." https://www.nist.gov/document/nicek12implementationplanpdf. Accessed January 4, 2021.

[5] Ing, M., Aschbacher, P. R., & Tsai, S. M. (2014). Gender Differences in the Consistency of Middle School Students' Interest in Engineering and Science Careers. *Journal of Pre-College Engineering Education Research (J-PEER)*, *4*(2).

[6] Bransford, John D., Ann L. Brown, and Rodney R. Cocking (2000). *How People Learn: Brain, Mind, Experience, and School*. Washington: National Academies Press.

[7] Noe, M. & Levin, L. (2020). Mapping the use of comics in health education: A scoping review of the graphic medicine literature. Graphic Medicine. https://www.graphicmedicine.org/mapping-comics-health-education/. Accessed January 4, 2021.

[8] Buchanan, L., Wolanczyk, F., and Zinghini, F. (2011). "Blending Bloom's Taxonomy and Serious Game Design." *Proceedings* of the 2011 International Conference on Security and Management, H.R.Arabnia, M.R.Grimaila, G. Markowsky, S. Aissi, Eds. CSREA Press.

[9] Buchanan, L. (2019, April 19). How do you create a branching web comic with Comic-BEE? [Blog post]. Retrieved from https://comic-bee.com/blog/how-do-you-create-a-branching-web-comic-with-comic-bee/.

[10] Katie Reynolds. (2019). 13 benefits and challenges of cultural diversity in the workplace. Hult Blog. https://www.hult.edu/blog/benefits-challenges-cultural-diversity-workplace/. Accessed January 4, 2021.

[11] Reed, J., Zhong, Y., Terwoerds, L., & Brocaglia, J. (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. *Frost & Sullivan White Paper*.

[12] Mountrouidou, X., Vosen, D., Kari, C., *et al*. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. In *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE* (pp. 157–176). Association for Computing Machinery. https://doi.org/10.1145/3344429.3372507

[13] Ladson-Billings, G. (2014). Culturally relevant pedagogy 2.0: aka the remix. Harvard Educational Review, 84(1), 74-84.

[14] Ross, Wilbur and Duke, E (May 2018). "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce". https://www.nist.gov/document/eowfreporttopotuspdf. Accessed January 4, 2021.

[15] Pruitt-Mentle, D., and Pusey, P. (2010). State of K12 Cyberethics, Safety and Security Curriculum in US: 2010 *Educator Opinion. Educational Technology Policy, Research and Outreach*.

[16] The EdWeek Research Center (2019). "The State of Cybersecurity Education in K-12 Schools: Results of a National Survey". https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf. Accessed January 4, 2021.

[17] Change the Equation (2014). Design principles rubric. Washington, D.C.

[18] Cyber Center for Education and Innovation. High School Cybersecurity Curriculum Guidelines. National Cryptologic Museum Foundation. https://cryptologicfoundation.org/what-we-do/educate/high-school-cybersecurity-curriculum-guidelines.html. Accessed January 20, 2021.

[19] Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and Cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. Journal of Digital Learning in Teacher Education, 28(2), 82-85.

[20] National Cyber Security Alliance, Microsoft Corporation, Zogby/463. (2011). The State of K-12 Cyberethics, Cybersafety, and Cybersecurity Curriculum in the United States.

[21] Inan, F. A. (2014). Cyber-Security Education for Community College Faculty in Texas-Final Evaluation Report. Lubbock, TX: Texas Tech University.

AUTHOR INFORMATION

Laurin Buchanan, Principal Investigator, Secure Decisions, Northport, NY. A Certified Information Systems Security Professional (CISSP), Laurin previously managed cybersecurity at several companies before becoming a researcher; she currently serves as co-chair of the NICE K12 Community of Interest.

Dr. Lori Scarlatos, Associate Professor in Technology and Society and affiliated with Computer Science and Institute for STEM Education (I-STEM), Stony Brook University, NY.

Nataliia Telendii, Ph.D. Candidate, Department of Technology and Society, Stony Brook University, NY.