Paper ID #25959

Design and Development of a Modular K-12 Cybersecurity Curriculum

Dr. Giti Javidi, University of South Florida

Dr. Giti Javidi received her BS from University of Central Oklahoma and MS and PhD from University of South Florida, Tampa. Prior to joining academia as a faculty, she worked for industry for several years including IBM as a software engineer. Dr. Javidi has more than 18 years of experience in teaching, research, industry and consulting services. She Joined USFSM IT program in fall 2016 as a n Associate Professor of Information technology and Cybersecurity, from Virginia State University (VSU) where she held the position of Professor of Computer Science. While at VSU, she played a pivotal role in developing and advancing the Computer Science program. She also provided IT training and consulting services to worldwide customers through her consulting company, Novus Kinesis. Dr. Javidi's research cuts across several disciplines within computer science, information technology, and education. Her research interests include human-computer interaction, user interface design, information visualization, and educational data mining. A unifying theme of her research is the focus on computer science and IT education. In recent years, while at USF, she has also been interested in IoT and Cybersecurity education. She is also very passionate about the role of women in IT. Dr. Javidi has received several prestigious awards. She was awarded the 2017 Women of Influence and 2018 Women in Leadership and Philanthropy award for her research. Dr. Javidi has been featured in Harold Tribune, Sarasota Magazine, Florida High Tech Corridor and several other venues. Her scholarly research has been published in peer-reviewed national and international journals and she has presented at several conferences and summits as an invited speaker. A long-time advocate for increasing participation and retention of women and marginalized population in STEM fields, Dr. Javidi has worked tirelessly on a number of projects in this domain over the past many years. In the recent years, she has been conducting research on exploring gender bias in IT and its impact on retention and recruitment in the field. She has been a longtime supporter of National Center for Women & Information Technology (NCWIT) and its mission, having spearheaded the establishment of an Academic Affiliation between NCWIT and VSU and most recently, USFSM. At the local and national level, she has collaborated with several organizations in their efforts to develop methods and strategies for increasing diversity in STEM. Dr. Javidi has been the recipient of a number of NSF, NASA, Google and Microsoft grants. She has also been a long time member of ACM and IEEE among a number other national and international organizations.

Dr. Ehsan Sheybani, University of South Florida

Dr. Ehsan Sheybani has earned BS, MS, and PhD in Electrical Engineering from UF, FSU, and USF respectively. His main research area has been applications of communication, signal processing, and data analysis. He has been involved in teaching, practicing, researching, and consulting applications of DSP in technology, system analysis, and data sciences for the past 20 years. He has a long list of publications and research grants including projects with NASA, NSF, NIH, DoD, DEd, and industry partners. Currently he serves as a faculty at the University of South Florida.

©American Society for Engineering Education, 2019

DESIGN AND DEVELOPMENT OF A MODULAR K12 CYBERSECURITY CURRICULUM

Abstract

This paper discusses an integrative model to raise interest among high school students in cybersecurity. As part of the model, several online modules have been created and tested by 30 high school teachers. An overview of the model and some of the findings regarding teacher perception of the modules and their preparedness to teach the content to their students are presented. This is an ongoing project with the ultimate goal of developing strategies for addressing shortage of cybersecurity workforce.

Keywords

K-12, Cybersecurity, Education, Workforce development, Teacher Education, Academic Engagement

1. Introduction

There is no dispute that cybersecurity professionals are needed in our growing economy. Despite this need, according to Bureau of Labour statistics [1], nearly 210,000 cybersecurity positions went unfilled in 2017 alone. This gap in cybersecurity workforce has left corporations in high demand for employees to meet security needs. The authors of this paper believe that the solution to this problem begins early in K-12. Early exposure to cybersecurity through a well-designed curriculum and set of activities will help alleviate the shortage by increasing the interest and skills of the new generation. Unfortunately, current secondary school curricula across the country leave students and educators with minimal or no exposure to cybersecurity topics. To address this need, we are proposing a model that can help narrow the cybersecurity workforce gap by introducing students to cybersecurity by building a pipeline towards cybersecurity careers for students and empowering teachers to integrate cybersecurity into their own classrooms and becoming advocates for cybersecurity awareness in their school districts.

Our long-term vision is to have cybersecurity taught at every high school using our modules as a standalone subject or to weave it into computer science courses, or AP courses in particular. The goal is to have every high school in the region establish cybersecurity clubs with diverse group of students and a teacher mentor who can provide them with the training to participate in local, regional and national cybersecurity competitions, and to raise parent and community awareness of security issues through k-12 schools. It is our hope that the activities planned and presented in the model will pave the path for reaching our ultimate goal of increasing the number of students interested in pursuing cybersecurity as a future career.

2. Cybersecurity Education in K-12

In response to the gap in cybersecurity workforce and talent, colleges and universities have started offering cybersecurity degrees [2]. However, it is our belief that a long-term solution to the cybersecurity workforce is to start educating students about those topics at early age. Surely the K-12 cybersecurity program should provide students with valuable learning experiences. 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 [3]. Cybersecurity awareness, education and training as defined by the National Institute of Standards and Technology (NIST) [4] are all important components of our model. NIST [4] defines "awareness" as teaching students about security concerns and threats and teaching them to respond accordingly. It also defines "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 accumulating 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 fulfil the role described by our definition, the proposed model provide activities applied to awareness, education and training.

In order to reach out to more high school students, we have developed short modules that can be injected into various courses (not just AP computer science). We believe that high schools should consider modules focused on cybersecurity as additions to Advanced Placement courses not only in Computer Science (where enrolment may be low), but also in other subject matters. These modules can also be injected into general courses in a variety of disciplines including the social sciences, psychology, and management science.

3. K-12 Cybersecurity Education Model

The goal of this project is twofold: (1) to increase the interest in cybersecurity workforce and (2) to increase the number of teachers equipped to embed the topics in their curriculum. As such, a model shown in Figure 1 is structured to address four critical areas that will help us reach those goals: 1) effective academic and social integration [5][6], 2) appropriate financial support, 3) narrow perception of the field of cybersecurity and available career paths, and 4) role models/mentors. The proposed model (Figure 1) is partly based on *Tinto's model of student integration* [5] which focuses more on experiences the students encounter after coming to college, rather than those occurring prior to college. But, we have found several aspects of the model that are also applicable to high school students such as retention in STEM areas and their transition to college in terms of staying interested in those areas.

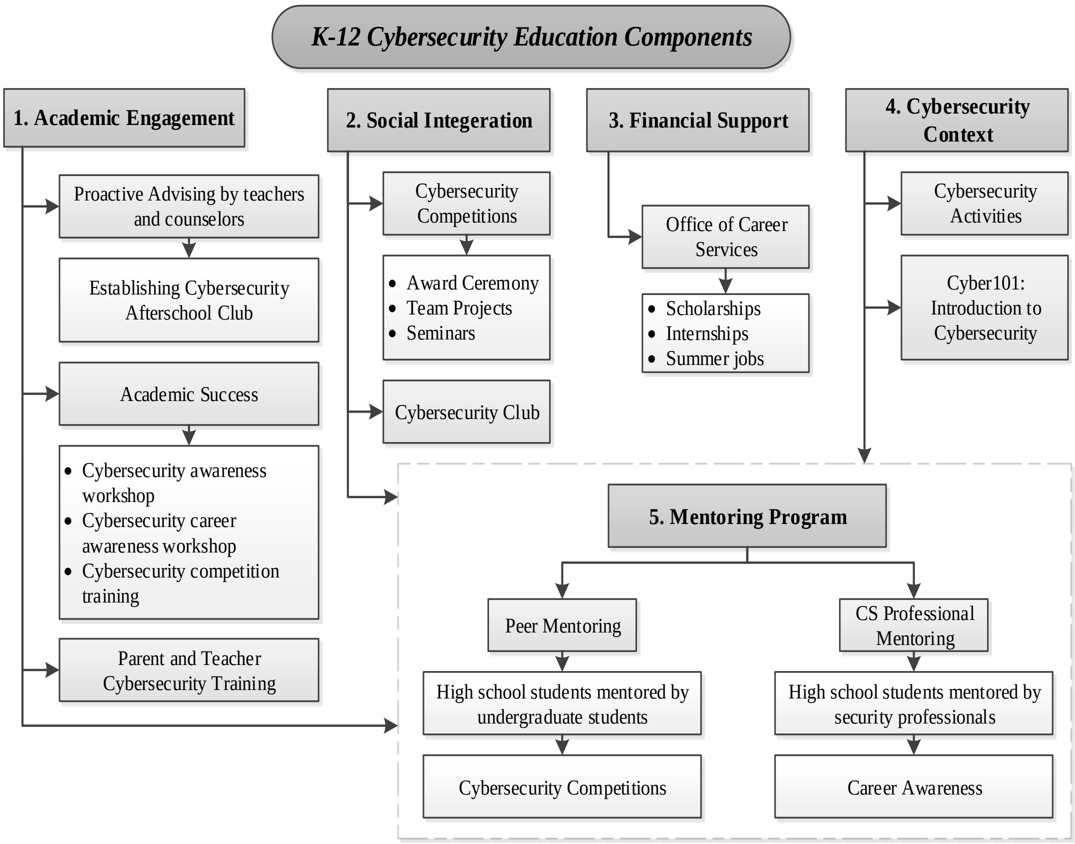
K-12 Cybersecurity Education Components
1. Academic Engagement
Proactive Advising by teachers and counselors
Establishing Cybersecurity Afterschool Club
Academic Success
Cybersecurity awareness workshop
Cybersecurity career awareness workshop
Cybersecurity competition training
Parent and Teacher Cybersecurity Training
2. Social Integration
Cybersecurity Competitions
Award Ceremony
Team Projects
Seminars
Cybersecurity Club
3. Financial Support
Office of Career Services
Scholarships
Internships
Summer jobs
4. Cybersecurity Context
Cybersecurity Activities
Cyber101: Introduction to Cybersecurity
5. Mentoring Program
Peer Mentoring
CS Professional Mentoring
High school students mentored by undergraduate students
High school students mentored by security professionals
Cybersecurity Competitions
Career Awareness

Figure 1. K-12 Cybersecurity Education Model

The five core components of this model are: 1) Academic Engagement, 2) Social Integration, 3) Financial Support, 4) Cybersecurity Context, and 5) the Mentoring Program, as shown in Figure 1. Each component of the model is described in greater detail.

3.1 Social Integration

With Tinto's theoretical framework in mind [5], to foster an increased sense of community between students, the model proposes several specific activities to be conducted throughout the year to enhance the social integration of students:

1. An orientation session specifically on importance of cybersecurity education to be held at the beginning of academic year. The session should focus on introducing students to the cybersecurity training/education opportunities, cybersecurity club, competitions, and mentoring opportunities
2. Award ceremony to be held at the end of each year to acknowledge the accomplishments of each student.
3. Award ceremony for the teachers who lead the cybersecurity initiatives in their schools.
4. Students should be exposed to non-academic support services such as guest speakers, undergraduate cybersecurity mentors, internship and summer program opportunities, and other means of getting advice about the field.
5. Social media groups should be created to encourage contact and communication among the students.

3.2 Academic Engagement

The model is based on Tinto's theoretical framework of student departure [5] which associates students' academic and social integration to their success in college. The argument behind Tinto's theory is that the more students are academically and socially integrated, the more successful they will be academically. Guided by the academic integration component of Tinto's theory of student departure, one integral component of the program is serious proactive advising. The goals of the advisement strategy is to have the high school and university advisors collaborate in promoting cybersecurity at the schools, identify interested students, maintain regular contact with students, facilitate the introduction of students to mentors and other available resources and monitor their progress. The idea is to follow up constantly with students. A checklist/rubric for advisors has been developed as a guideline to help with a consistent way of advising.

3.3 Financial Support

Clearly a key element of college attendance for many students is the financial support. The sobering reality of high cost of attending college has led many of the high school students to take a serious look about the value of a college degree and instead pursue other opportunities after graduation. Therefore, this is a critical time for all educational entities to look deep into the educational practices and reform the education system to build programs that prepare students for skills that are needed for high demand professions into their core curriculum. These programs should take into account the marvels of cybersecurity education for building meaningful experiences for students. Therefore, as part of this model, we propose the importance of financial support and financial aid to help more students have the opportunity to attend college and gain more knowledge and skills to pursue degrees in cybersecurity and related fields.

3.4 Cybersecurity Context

In order to ensure that students have a proper concept of what cybersecurity is and are aware of career opportunities in this field, the following specific activities should be performed:

1. Students should be exposed to information about the broad field of cybersecurity and range of industry positions, thus dispelling myths about the field.
2. The authors of the paper have developed a course *Cyber101* as an online course with six modules, as a teaching tool for high school teachers. The modules can be embedded into any subject matter or weaved into AP Computer Science course.
3. Industry guest speakers can be invited to the schools to give students a better idea of what the day-to-day activities of cyber professional may encompass. Students should also have field trips to cybersecurity facilities. Universities have the means to capitalize on their industry partnerships to help high schools identify relevant locations to visit.

3.5 Mentoring Programs

The model is proposing a mentoring program designed to assist high school students and teachers with competition preparations. The mentors will meet with mentees on regular basis to give them support and. We are hoping that the mentoring groups will give students an instant group of friends and cyber enthusiasts. Students should also have access to cybersecurity practitioners. This relationship will be crucial since the mentors will serve as role models and provide crucial advice and support. The mentoring program will be optional for the students, but strongly encouraged. This can be achieved by creating an environment where school districts, high school teachers, university faculty, and industry professionals can work together to offer the best learning experience to students.

The five core components with the interventions and outcomes are explained in more detail in Table 1.

Table 1. Summary of critical areas, interventions, and objectives

Critical Areas	Interventions [with High School and University Partner(s)]	Objectives
Academic engagement	• Proactive advising Awareness/training/career seminars • Peer mentor workshops • Cyber101 course • Embedding cybersecurity modules into all other subjects • Weaving cybersecurity modules into AP CS course • Teacher cybersecurity training • Parent cybersecurity training	• Increased interaction between universities and high schools • Greater student knowledge of and interest in cybersecurity topics and careers • Increased number of teachers leading cybersecurity education in their schools • Increased parent awareness of cybersecurity topics • Increased sense of responsibility to act as a human firewall
Social integration	• Peer mentor interaction • Social activities via student clubs • Team cybersecurity projects • Awards ceremony • Cybersecurity events and competitions	• Greater student participation in cybersecurity competitions • Increased sense of belonging within the field • Increased interaction with mentors • Increased confidence about cybersecurity skills in in social and professional situations • Increased security awareness • Increased sense of urgency in increasing cybersecurity workforce
Financial support	• Scholarship Opportunities • Summer Internship	• Meet financial needs to complete computer science

	Opportunities • Job Opportunities	degree • Gain cybersecurity experience while getting paid during summer
Perception of the cybersecurity field and career paths	• Career seminars • Cybersecurity club • Field trips to company visits • Industry and university guest speakers • Monthly cybersecurity newsletter	• Increased number of students who want to pursue cybersecurity • Broadened exposure and understanding of cybersecurity and associated career paths.
Role-models/ mentors	• Student and Professional mentors	• Offer visibility of and opportunity for networking • Increased opportunity for mentees to acquire new knowledge and skills by understanding the mentor's practical experience • Increased motivation by breaking-down stereotypes about who can be successful in cybersecurity.

4. Teacher and Parent Training

The cybersecurity 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. In the field of cybersecurity, this issue becomes more trivial since organizations can’t afford to underestimate their exposure to cyber-attacks and the importance of cybersecurity. Increasing cybersecurity professionals is a necessary solution to the cybersecurity skills crisis in the technology industry. One way to ensure a larger pipeline in cybersecurity is to train more high school teachers to not only teach cybersecurity in their schools and/or integrate cybersecurity concepts in their classrooms but also to promote IT security as an attractive career path. The gateway to our next, best generation of tech-savvy workforce is training high-quality teachers since they are the most powerful component in influencing and controlling a student's educational route. According to Sidik [7] “while other social factors (peers, parents and teachers) have been stressed as vital stimuli on students’ impending choices, students’ dislike of STEM careers can be linked to dissuasion experienced in their K-12 years [7]”. Teachers are remarkably well positioned to be role models that touch students’ attitudes, interests and career choices [8]. The literature suggests that K-12 schools need teachers as role models who can move them toward a STEM career. More teachers with positive STEM attitude are needed to understand students’ defiance about the subject with the intention to positively influence it [9] [10]. It is also evident in our previous work that “empowering teachers with computing skills and tools will impact students’ perception of computing as career [11]”.

All the workshops that we have been conducting have been based on the notion that “it takes a village to raise a STEM-ready talent”. We need everyone including parents, teachers and the community to raise techie kids. Many times parents are an untapped resource for encouraging children to pursue STEM studies. Parents can make a huge difference. What parents say or do can influence how their children see themselves and their ability to succeed in a STEM career. A simple encouragement from family members can drive STEM interest in children. Parents can instil in their children the self-confidence needed to rebound from a failure. But, many times they do not know much about STEM, existing fields within STEM and the tools available which can be used to expose their kids to the broader world of science and technology. These children also get to see their teachers every day, hence those teachers have a responsibility to raise their confidence in their abilities. However, in order for teachers to successfully implement cybersecurity or any STEM-related subject in their schools, they need “STEM-interested” student body, which can potentially have significant long-term implications in increasing cybersecurity pipeline. We have conducted several workshops engaging parents alongside their 9th-11th grade children and their teachers in coding and cybersecurity awareness. This has been part of an effort to invite parents and teachers to join in the effort of bringing coding and cybersecurity to their schools, homes and their family conversations. So far In addition to these teachers, 65 parents alongside their children have completed workshops on coding and cybersecurity awareness but this paper will report only the results of the teacher preparation.

4.1 Teacher Training Findings

The authors have created several modules in cybersecurity and have offered several workshops. As an initial pilot test of the modules, we offered a one-week summer program for high school teachers. The aim of the program was to train teachers in using the curriculum while getting feedback about the quality of the modules and help them to bring cybersecurity projects, technology, and curriculum into their classrooms, assist teachers with mapping cybersecurity modules, lesson plans and topics to their curriculum, create awareness among the teachers about the importance of cybersecurity and their role in students’ attitude towards cybersecurity career, introduce teachers to various careers/areas in cybersecurity, and introduce creative ways to get teachers engaged in use of the tools in their teaching.

Thirty 9-11th grade teachers were recruited from local high schools and participated in a one-week, 40-hour, workshop to receive instructions on cybersecurity awareness and various other topics using the modules developed by the authors. In addition, one cybersecurity practitioner was invited as a guest speaker to discuss careers in the field. A pre and post-survey was administered at the completion of the workshop to gather data about teachers’ perceptions, understanding, and practices with regard to several key topics. Participating high school teachers taught subject areas which included reading, math, science, social studies, technology or technology education, English, AP computer Science, and foreign language. Two of the teachers had at least a master’s degree, and their years of teaching experience ranged from 3 to 16 years.

Teacher’s perception about the value of cybersecurity education and the support they receive for incorporating security topics in their classroom were measured in a survey asking teachers to respond on a 4-scale with their level of agreement (strongly agree to strongly disagree). In general, the level of interest, perception, confidence, and motivation of teachers was significantly improved after this training workshop. More teachers reported being more prepared to teach basic cybersecurity contents in their classes given that they would have access to the modules. As such, 27 out of 30 claimed that they are ready to teach basic cybersecurity concepts. All teachers, except 2, reported that they feel equipped to talk to students about protecting their safety and privacy online and about cyber bullying. When asked about support they receive from their schools to incorporate cybersecurity into the curriculum, the teachers reported that the support is not available. For instance only 2 teachers agreed with the item "There is incentive from my school for me to make any extra efforts to include this topic in my lessons", and 3 teachers agreed with the "I have support in my school to modify the curriculum to incorporate cyber security topics in my lesson plans." The teachers were also asked to rate the availability of resources in their school. On the question of "When it comes to children online, it should be up to parents, not teachers, to teach cyber safety, cyber bullying and cyber security," all teachers except 4 agreed with the item. Also, on the item "My school/school district does an adequate job of preparing students regarding cyber ethics, online safety, and computer security issues," only two people agreed.

The results indicate that the only solution to teachers being able to promote cybersecurity topics in their schools is to get support from their schools which according to the results is not available. Teachers seemed to have a good understanding of the basic cybersecurity awareness topics. Also majority of them agreed that cybersecurity awareness starts at home and is parents' responsibility but it also has to start at elementary school. They also reported that they had a good understanding of cybersecurity careers. Overall, the teachers reported positive reactions to the usability of the modules. They viewed it as a beneficial opportunity. They believed that the modules equipped them with tools that could help them in promoting cybersecurity at their school.

5. Conclusions

As a result of this model and the associated and the preceding IT preparedness modules, this project has trained 30 teachers from different disciplines in basic IT and cybersecurity concepts. The topics cover a wide range from awareness and responsiveness to coding and troubleshooting. Only one teacher has incorporated this model at her school by revamping the curriculum at the school level. Other teachers have only incorporated parts of the model (modules) in their curriculum. As a result of this study, we have spotted the obstacles blocking the process and have been working and planning with school district administrators to resolve existing issues. It is our belief that empowering teachers with cybersecurity skills and tools will impact students' perception of cybersecurity as a career. The project seems to have been successful in increasing teacher's skills and knowledge in cybersecurity. The goal of this project was (1) to increase the interest in cybersecurity workforce and (2) to increase the number of teachers equipped to embed the topics in their curriculum. As such, a model was discussed to address four critical areas that will help us reach those goals: 1) effective academic and social integration, 2) appropriate financial support, 3) narrow perception of the field of cybersecurity and available career paths, and 4) role models/mentors. The modules developed for the academic engagement section of the model was well-received by the teachers who participated in a one-week summer program. Our hope is that the model can be used to increase teachers' and students' interest in cybersecurity, thus, providing the social and academic support to keep students interested in the field in their transition from high school to college. Also on-going professional mentoring provides crucial advice and moral support to help the students persist and succeed in the field. Together, these activities not only help students develop better self-confidence and persist in cybersecurity but also provide them with educational experiences that leverage them into cybersecurity related fields in college.

ACKNOWLEDGEMENTS

This material is based upon work supported by Google CS4HS and NCWIT. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Google or NCWIT.

REFERENCES

[1] Bureau of Labor Statistics, U.S. Department of Labor, "Occupational Outlook Handbook, Information Security Analysts." 2018. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm [Accessed May 31, 2018].

[2] K. Cabaj, D. Domingos, Z. Kotulski and A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs", *Computers & Security*, Vol. *75*, pp 24-35, 2018.

[3] R. Reid and J. Van Niekerk, "Snakes and ladders for digital natives: information security education for the youth", *Information Management & Computer Security*, Vol. 22, No. 2, pp 179-190, 2014.

[4] 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

[5] V. Tinto, A. G. Love and P. Russo, *Building Learning Communities for New Students: A Summary of Research Findings of the Collaborative Learning Project.* University Park, PA: National Center on Postsecondary Teaching, Learning, and Assessment, 1995.

[6] F. Hrabowski, "Raising Minority Achievement in Science and Math," *Educational leadership*, pp. 44-48, 2013.

[7] O. Sadik, O., "Encouraging Women to Become CS Teachers", *Proceedings of the 3rd Conference on GenderIT*, pp. 57-61, 2015

[8] M. M. Habashi, W. G. Graziano, D. Evangelou and I. Ngambeki, "Teacher Influences on Child Interest in STEM Careers*", Proceedings of the Research in Engineering Education Symposium 2009*, Palm Cove, QLD, 2009

[9] K. Kiili, "Digital game-based learning: Towards an experiential gaming model." *The Internet and Higher* Education, Vol. 8, No. 1, pp. 13-24, 2005.

[10] L. Pollacia and W. Lomerson, "Analysis of factors affecting declining CIS enrollment", *Information Systems, International Association for Computer Information Systems*, Vol. VII, No. 1, pp. 220-225, 2006.

[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.