Open Access License Notice

Improving the Pipeline

Sandra Gorka
Pennsylvania College of Technology
Williamsport, PA, USA
sgorka@pct.edu
cyber.pct@gmail.com

Alicia McNett
Pennsylvania College of Technology
Williamsport, PA, USA
amcnett@pct.edu

Jacob R. Miller
Pennsylvania College of Technology
Williamsport, PA, USA
jmiller3@pct.edu

Bradley M. Webb
Pennsylvania College of Technology
Williamsport, PA, USA
bwebb@pct.edu

***Abstract*—There is currently a shortage of cybersecurity professionals worldwide. This paper presents an after-school program for high school students to explore cybersecurity topics and careers. The paper discusses the content of the course as well as the results that have been seen to date. A link to an online repository of program materials will be shared with the audience. This work effort is the result of the NSF funded grant Improving the Pipeline: After-School Model for Preparing Information Assurance and Cyber Defense Professionals (Grant No. 1623525).**

Keywords—computing education programs, K-12 education, security and privacy

I. Introduction

There is currently a shortage of cybersecurity professionals both worldwide (estimated 2.9 million) and in the U.S. (estimated 498,000) [1]. Additionally, there is a skills shortage in cybersecurity that is impacting the U.S. [2]. Improving the Pipeline is an NSF funded grant (Grant No. 1623525) to extend the information assurance and cyber defense pipeline into the high school environment by offering an opportunity for high school students to enroll in an introductory cybersecurity course.

Section 2 of this paper discusses the motivation and goals of the grant. Section 3 discusses the format and content of the course developed and offered to the high school students. Section 4 discusses some lessons learned as well as summarizes collected data from students. Section 5 provides a mechanism through which readers can obtain educational materials developed for the course. Finally, Section 6 discusses the future of the course.

II. The Grant

The goal of this grant was to increase the capacity of educational institutions to produce more Information Assurance and Cyber Defense (IA/CD) professionals by developing a model for a high school after-school college-credit bearing program that 1) raises awareness about cybersecurity careers, 2) generates interest in those careers, and 3) prepares students to pursue the education required to succeed in cybersecurity fields [3].

The project developed and offered an after-school course that was offered during the 2017-18 and 2018-19 academic years. A total of 40 students from four local high schools participated in the year-long course over the two academic years.

III. The Course

A. Course Format

This 4-credit course was offered as a year-long course in which students attended class on campus once per week for approximately two hours – the equivalent of 2-credits in each of the fall and spring semesters. Two sections of the course were offered each year – one immediately after-school and the other later in the evening. Although students were assigned a specific session to attend, faculty were flexible enough to allow students to attend either session – providing more flexibility for students to participate in high school activities.

Based on feedback from the students, the after-school format was more desirable than running the course as a summer camp. The students felt this was less intrusive to their summer vacation and/or summer job. The early and late after-school timeframes supported students who had commitments immediately following school (e.g. band, sports, etc.). The early after-school timeframe supported coordinating transportation to the college for the students following the school day and to home at the end of class.

B. Course Content Selection

This section discusses the motives for selecting topics for this course. Our basic design philosophy for course content begins with the stated purpose of The National Strategy to Secure Cyberspace from February 2003: "to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." [4] To this end, we wanted the grant class to be a foundation for cybersecurity for those students who planned on a career within the computing discipline. At the same time, we wanted the class to provide the sufficient background that would allow anyone completing the class, to understand why cybersecurity is important, to be able to secure their own systems and to be a security-minded professional in whatever career they chose.

Another primary goal was that students who successfully completed the coursework would receive credit for Penn College's 3-credit CIT230 Fundamentals of Security course. The CIT230 course is a general introduction to security course taken by all of the college's information technology students. The CIT230 course strives to provide all information technology students with the cybersecurity foundation necessary for a successful career in whichever

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

specialization a student selects. As a result, the course content for the grant mirrors the content of the CIT230 course.

The original content of the CIT230 course dates back to 2003 when we developed our first information assurance and security program. At that time, the primary documents used for the content of the course included NSTISSI 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals [5] and a draft volume of IT2008 [6]. The content of NSTISSI 4011 was separated into two classes the CIT230 class and a class on penetration testing. Security content from the draft volume of IT2008 was also added to the CIT230 class.

Since our initial development of the CIT230 class, faculty continue to monitor curricula recommendations and the computing landscape to improve, not only CIT230, but the program as a whole. As such, there are many documents and events that have contributed to updates to CIT230 and our program; including, but not necessarily limited to:

1. National IA Education & Training Programs [7]
2. NICE Framework [8]
3. Cybersecurity Curricula 2017 [9]
4. Information Technology Curricula 2017 [10]
5. ABET Criteria for Accrediting Computing Programs [11]
6. Recommendations from our industrial advisory committee and graduates
7. Discussions with industry professionals at conferences
8. Current news and trends in the industry

It is also noted that the prerequisites of CIT230 include one semester of programming and one semester of networking. Since the class developed for the grant assumes no to minimal previous instruction in information technology, basic knowledge of programming and networking concepts were included in the course. The focus of this knowledge is to provide the foundation to better understand the security risks associated with software and networks and to develop a basic understanding of why certain mitigations can minimize the risk.

C. Course Content

The course topics were selected to give students perspective on the breadth of IA/CD careers. To the extent possible, topics were arranged in self-contained modules. Exceptions include introductory modules on the basics of security as well as network and programming concepts. The basics of security module (or portions of it) includes prerequisite knowledge to most of the other modules. The network concepts module contains prerequisite knowledge for the modules on network security as well as wireless security; the programming concepts module contains prerequisite knowledge for the security by design module.

Module names and descriptions follow:

0. Basics of Security – provides an introduction to the concepts of data and information as well as confidentiality, integrity and availability of data and information
1. Basics of Computing – provides a discussion of some basic computing concepts; labs include installing operating systems, adding/removing software and connecting hardware.
2. Programming Basics – provides an introduction to fundamental programming concepts, syntax and structures; labs include writing simple programs with input/output as well as basic control structures.
3. Security by Design – provides a discussion of how to prevent common software design flaws that facilitate insecure application behavior; labs include activities that utilize run-time errors, data validation, and SQL injection.
4. Basics of Networking – provides an introduction to fundamental network concepts including protocols and hardware; labs address network protocols and addressing, connecting hardware.
5. Network Security – provides an introduction to securing the perimeter of an information system; labs include protection of data in transit, authentication and access controls; performing network scans to find vulnerabilities.
6. Wireless Security – provides an introduction to secure wireless communications; labs include comparing wired and wireless connection; using Wireshark and securing wireless connections.
7. Encryption: Protecting Confidentiality – provides an introduction to the use of encryption to protect confidentiality of information assets; labs include using simple ciphers and encrypting/decrypting files.
8. Hashing: Protecting Integrity – provides an introduction to hashing algorithms and using them to ensure integrity; labs include viewing stored (and hashed) passwords, validating file content using hash signatures, identifying modified data using hash signatures.
9. Protecting Availability – provides a discussion of denial of service (DoS) and how to prevent it; labs include understanding how DoS attacks work, limiting the effects of DoS attacks and Bots and BotNets.
10. Social Engineering – provides a discussion of the art of compromising the human; labs include methods to protect yourself, phishing attacks and developing a trust but verify attitude.

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

11. Risk – provides an introduction to stakeholders, information assets, threats and vulnerabilities as well as risk assessment and management; labs include activities to identify stakeholders, assets and threats, assessing the risk and managing the risk through recommending transference, acceptance, avoidance and mitigation.
12. Policy, Legal Issues and Professionalism – discussion of policy and the legal/professional issues associated with IA/CD as well as repercussions of cybercrime.
13. Contingency Planning – discusses the idea that even the best security can fail and what to do when it does; labs include discussions of situations where security fails and what can be done to plan for such events.

D. *Module Format*

Each of the mentioned modules was developed in a consistent manner and focused on identifying "security decision-making considerations". Each module begins with a discussion of these considerations in an effort to provide a consistent method of introducing each module [12].

The security decision-making considerations, along with a brief description of each, follow: [12]

- Risk –What is the risk of failing to protect the information/data from threats?
- Controls – What methods can a user/professional put in place to lessen the risk of the harm identified above?
- Who cares – Is the risk associated with a person, overall business, government, etc.? Should I be concerned about this risk or is someone else concerned for me?
- Who implements/manages – Who/what jobs involve implementing the identified controls?
- What is protected – What is the data or information asset that must be protected?
- When must it be protected – Does the information need to be protected at rest, in transit, both, etc.?
- Where can it be protected – Do we need hardware/software protections? What types of devices need to be protected?
- How can it be protected – What are the specific actions/controls that can protect the information/data from a given threat?
- Why is it important to protect – What are the benefits of protection versus the impacts of compromise of the information/data?

IV. Results

Prior to beginning the program, a math placement exam was conducted. The initial review of the raw data indicated that an overall high school freshman level of math was largely a sufficient prerequisite for the program. However, when reviewing overall student performance (e.g. final grade), individual math placement did not appear to be a predictor of student performance (see Figure 1).

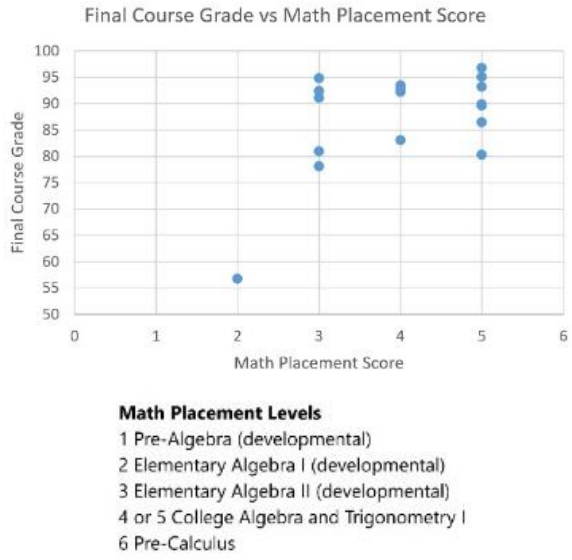

Fig. 1. Comparison of math placement exam scores and final course grade.

Reading comprehension testing also took place before the program started. The raw data appeared to show a correlation to overall student performance in the program. The students with a lower than expected reading comprehension level did not perform as well as their peers (see Figure 2).

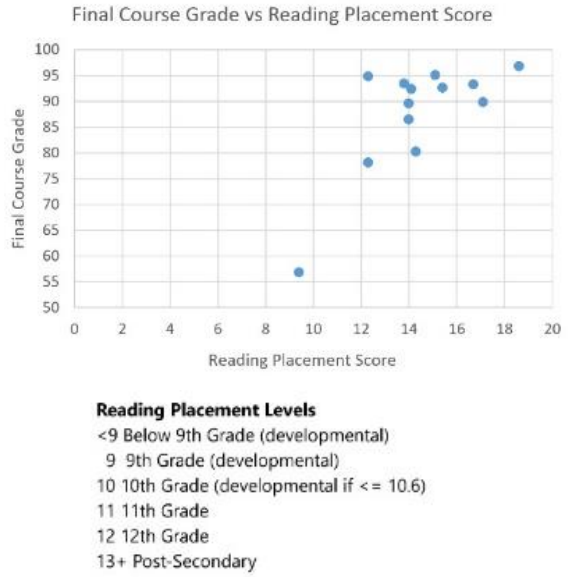

Fig. 2. Comparison of reading placement exam scores and final course grade.

Pre- and post-module surveys were conducted for each of the modules. The surveys were used to gauge student comprehension of each module topic area, determine the impact of module materials, and assess overall student satisfaction with the module. While data collection is currently on-going, preliminary raw data collection has begun to yield some evidence. When testing incoming student knowledge, the modules that indicated lower comprehension levels included:

- Programming Basics
- Security By Design
- Encryption: Protecting Confidentiality
- Basics of Networking
- Hashing: Protecting Integrity
- Protecting Availability
- Risk
- Policy
- Contingency Planning

Modules with higher scores indicating higher incoming comprehension levels included:

- Basics of Security
- Social Engineering

Pre- and post-assessment averages of each module are presented in Figure 3.

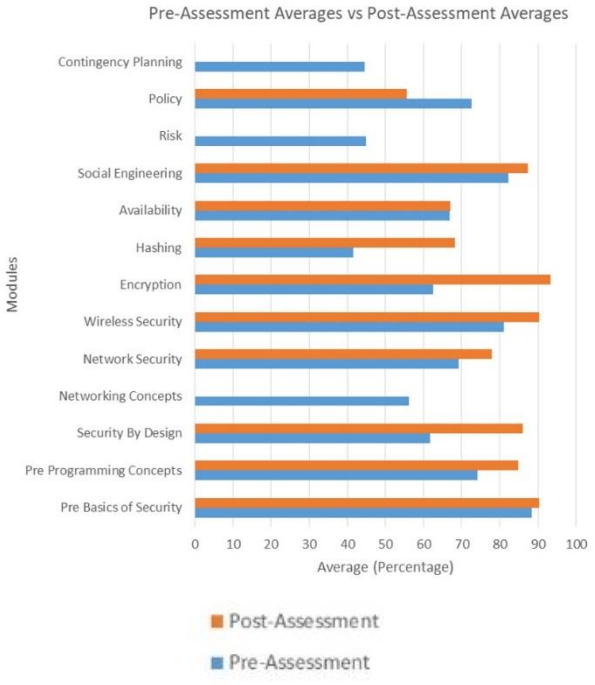

Fig. 3. Comparison of pre- and post- assessment averages.

V. Accesing the Course Materials

Some of the instructional activities used during the course were acquired through a Creative Commons Non-Commercial License. As such, while materials are freely available for your use, we ask that you publicly give credit for the development of these materials.

Some activities within the modules were adapted from the Create Commons. This is indicated within the modules and should be acknowledges as a work licensed under a Creative Commons Attribution – NonCommercial-ShareAlike 4.0 International License.

This project was supported by the National Science Foundation and materials developed for the grant are available via Google Drive. Individuals requesting access will be asked to complete a survey. The survey will be used to track dissemination of the materials for grant reporting purposes. Access will be granted once a survey is completed to track dissemination of materials.

Individuals interested in obtaining access can be requested manually by emailing a request to cyber.pct@gmail.com. Once a request is received, a reply will be sent that includes a link to the google survey. Alternatively, individuals will be granted access upon completion of the survey found at

https://docs.google.com/forms/d/1lqdLyQADO_v7WA5o3tTggkGco5eKyhb_t80N82ZDj1Y/edit?usp=sharing.

Issues encountered while accessing the materials should be directed to cyber.pct@gmail.com.

VI. The Future

We have learned several valuable lessons as we look towards the future. First, through an analysis of the math background of the two cohorts and their academic success, we have determined that students can comprehend this material with more basic math skills than typically expected of computing students. Our analysis shows that students with the equivalent of 11th grade math are capable of succeeding in this course.

Second, while the course was envisioned to help encourage students to pursue a career in IA/CD, it may have been more successful in preparing individuals to be "cyber-safe". Some participants have indicated that the course opened their eyes to a new career field, but more indicated that the lessons would serve them well in other college majors/professions. Students report being more concerned/cautious with their online presence, educating their family and friends about social engineering pitfalls, and having a greater appreciation of the multiple cybersecurity concerns businesses and individuals face each day.

Combined, these two lessons have adjusted our outlook on how to craft a sustainable product from the work on this grant. Instead of focusing on creating future IA/CD professionals, the better course of action is to increase cybersecurity awareness and training in more individuals. Due to this, we have adjusted the course described previously

in this paper to be an introduction to cybersecurity for non-IT majors. The math level is lower than required for IT majors, and the credit load is now three.

This revised course (CSC229) is now listed in the Penn College catalog and available for any student at Penn College to take. We have already seen interest in the business and nursing programs to require this material. Additionally, we always had the intention of allowing this course to be offered in our dual enrollment format. Based on accreditation standards, this requires a high school teacher to present the content. We had concerns about the content knowledge of a typical high school technology teacher. By reducing the credits and re-envisioning the course to be more accessible to all majors, it should also be easier to find qualified high school instructors.

While the implementation of this project was possible due to funding from the NSF, the intention was always for it to be continued beyond the conclusion of the grant. As such, the grant period has allowed us to try out new techniques, develop new labs, and investigate teaching methodologies that would work well with high school students, as well as those who are not interested in pursuing a career in a computing discipline. In the end, we have learned that the material can be presented to younger audiences and across disciplines in a meaningful way. The future of this program resides in enabling individuals to be "cyber-safe". To facilitate this, we will be teaching a dual enrollment course CSC229 – Introduction to Cybersecurity for Non-IT Majors, beginning with the Fall 2019 semester.

Acknowledgements

This material is based on work supported by the National Science Foundation under Grant No. 1623525. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Barker, I. (2018, October 17). Cybersecurity faces a worldwide shortage of almost 3 million staff. betanews. Retrieved November 18, 2018, from betanews: https://betanews.com/2018/10/17/cybersecurity-worldwide-skills-shortage/.

[2] Security Magazine. (2018, June 6). US Cybersecurity Worker Shortage Expanding. Retrieved November 18, 2018, from https://www.securitymagazine.com/articles/89087-us-cybersecurity-worker-shortage-expanding.

[3] Sandra Gorka, Alicia McNett, Jacob R. Miller, Bradley M. Webb. 2017. Improving the Pipeline: After-School Program for Preparing Information Assurance and Cyber Defense Professionals. In Proceedings of SIGITE'17, Rochester, NY, USA, October 4–7, 2017, 1 pages. https://doi.org/10.1145/3125659.3125665.

[4] United States. Department of Homeland Security. (2003). The National Strategy to Secure Cyberspace. https://www.hsdl.org/?abstract&did=1040.

[5] NSTISSI (1994). National Security Telecommunications and Information Systems Security Instruction No. 4011. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf.

[6] Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. (2018) ACM/IEEE-CS. Retrieved from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2008-curriculum.pdf.

[7] National IA Education & Training Programs, Found at https://www.iad.gov/NIETP/CAERequirements.cfm.

[8] National Institute of Standards and Technology Special Publication 300-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, August 2017. https://doi.org/10.6028/NIST.SP.800-181.

[9] Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. (2017) ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8. Retrieved from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

[10] Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology. (2017) ACM/IEEE-CS. Retrieved from: https://www.acm.org/binaries/content/assets/education/curricularecommendations/it2017.

[11] ABET Criteria for Accrediting Computing Programs; https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2020-2021/.

[12] Gorka, S., & Miller, J.R. (2019, January 20). Kinder Garten Security: Teaching the Pre-college Crowd. *ShmooCon Presentations*. Washington D.C.: Shmoo Group. Retrieved from http://archive.org/details/ShmooCon_2019/ShmooCon2019-Kinder+Garten+Security.mp4