Cybersecurity

at Columbus State

Columbus State Community College Cybersecurity Program Final Evaluator's Report

Summer 2019

Prepared By:
UW Stout Applied Research Center

Prepared For:
Columbus State Community College

Authored by staff at the UW Stout Applied Research Center, supervised by Justin Sullivan, M.S.

This material is based on work supported by the National Science Foundation NSF Proposal #1501194. The opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not reflect the position or policies of the National Science Foundation.

Table of Contents

Index of Tables

Acronyms:
CSCC: Columbus State Community College
NSF: National Science Foundation
ATE: Advanced Technology Education

Columbus State Community College Cybersecurity Program

Evaluators Report

Overview

Columbus State, in collaboration with Franklin University, NSF ATE National Cyber Watch Center (Prince George's Community College), Columbus City Schools, Reynoldsburg City Schools, and key industry partners (E&Y, Abercrombie & Fitch, Alliance Data, Ohio Health, Nationwide, The Columbus Collaboratory, and Tech Columbus – now Rev1Ventures) researched and developed an academic and career pathway in Cybersecurity education as supported by grant funding provided by the National Science Foundation (NSF). Instructional and student support systems were developed to help establish the optimal environment for student success. The overall project goal was to create a career pathway for Cybersecurity professionals with subject matter knowledge and industry input to support the increasingly complex technology needs within security while providing program graduates opportunities in a variety of industry and government entities. The project worked to achieve this goal by creating an Associate Degree curricula in Cybersecurity, developing a Cybersecurity Pre-College Initiative, and forming a University articulation for Cybersecurity.

The purpose of this report is to evaluate the degree to which this program has met its intended goals and is primarily produced for project staff and funder reporting.

Methodology

The goal of the CSCC training pipeline in Cybersecurity project is to establish a Cybersecurity Training Pipeline in the Ohio region to increase the supply of qualified cybersecurity professionals for industry and government.

Industry employers were asked to provide input as to the knowledge, skills and abilities that would be desirable among entry level employees in cybersecurity. At the institutional level, institutional data was used to monitor student outcomes related to enrollment, retention, transfer rates, and grades. This allowed for comparison among students in the newly established cybersecurity program and other computer science programs, and all programs at CSCC. Students were also asked to complete an exit survey upon leaving the program. This survey was designed to measure a student's satisfaction with the program and to also gage employment outcomes as reported by the student. Finally, to foster a spirit of sustainability, a group interview was held among those who were involved in the initial grant work, developing curriculum and ultimately creating the program.

The results are listed below.

Results

Industry Engagement Survey

A survey was designed to capture the preferences and concerns among potential employers of graduates of the Cybersecurity program was administered by the Applied Research Center. The results are summarized below. Appendix A contains a copy of the survey.

1. **Expertise of Entry Level Cyber Security Professionals**
   Areas rated for level of expertise:

a. Secure Provision: Respondents indicated Proficient or Master levels 75% (N=3) were needed for Systems Security Architecture. Respondents indicated Component or Proficient levels 100% (N=4) were needed for Software Assurance and Security Engineering.
b. Analyzation: Respondents indicated Competent or Proficient levels 75% (N=3) were needed for Cyber Threat Analysis and Exploitation Analysis. Respondents indicated Novice and Competent levels 75% (N=3) were necessary for All Source Intelligence Target.
c. Collect and Operate: Respondents indicated Competent or Proficient levels 75% (N=3) were needed for Cyber Operations and Novice or Competent levels 100% (N=4) were needed for Operations Planning and Collection Operations.
d. Protection and Defense: Majority of respondents 75% (N=3) indicated Proficient levels were needed for Computer Network Defense (CND) Analysis and Computer Network Defense (CND) Infrastructure Support. Respondents indicated Competent or Proficient levels 100% (N=4) were needed for Incident Response and Vulnerability Assessment and Management.
e. Investigation: Respondents indicated Competent or Proficient levels 100% (N=4) were needed for Investigation. Whereas, 75% (N=3) of respondents indicated only Competent levels were needed for Digital Forensics.
f. Oversight and Development: Respondents indicated Novice levels 50% (N=2) were needed for; Strategic Planning and Policy development, Security Program Management (CISCO), Information Systems Security Operations (ISSO), and Education and Training. Majority of respondents 75% (N=3) indicated Novice levels were needed for Legal Advice and Advocacy.
g. Operation and Maintenance: Respondents indicated Proficient or Master levels 100% (N=4) were need for System Administration. Majority of respondents, 75% (N=3) indicated Proficient or Master levels were needed for Network Services. In addition, 75% (N=3) indicated Proficient levels were needed for Systems Security Analysis and Customer Service and Technical Support.

Areas of expertise ranked in the cyber security industry:

a. Half of the respondents 50% (N=2) ranked Certifications as the most important area of expertise. Half of the respondents 50% (N=2) ranked the least important areas as Networking.

2. Interest with Other Cyber Security Organizations

a. Collaborating on projects and partnerships
    - All the respondents 100% (N=4) indicated they are interested in collaborating on projects with other cyber security organizations. All the respondents 100% (N=4) indicated they are interested in partnerships with other cyber security organizations.

3. Hiring of Computer Science Graduates

Frequency of hiring cyber security professionals:

a. When participants were asked, "How frequently does your organization hire any type of cyber security professional?" Half of the respondents 50% (N=2) indicated Infrequently and 50% (N=2) indicated Frequently.

Appendix B contains a full report summarizing results for each question.

Institutional Student Data

Success of institutions of higher education is measured across many variables. The standardized method in which data are collected makes it possible to compare benchmarks among institutions at the Federal level. The National Center for Education Statistics uses the following major data points for comparison: enrollment,

applicant data, transfer in and out rates, grade point average (GPA), and graduation rates. As a benchmark of success these data were collected from Columbus State Community College at the college level, the computer science (subject) level, and at the program level (Cybersecurity) level. The results are presented below.

The data below reflects student enrollment for the 2016-2017 and the 2017-2018 academic school years as measured in the fall semester. Enrollment data typically follows a fall to fall comparison. Data is not yet available for the 2018-2019 academic school year.

Table 1 displays application data for Columbus State Community College at the college, subject and program level for Cybersecurity.

Table 1: Application Data

	FA16	FA17	FA18
Overall CSCC	18,643	20,815	20,917
CSCC Computer Science	550	646	907
Cybersecurity	*	174	86

**Data not available*

Table 2 displays enrollment data for the Cybersecurity program. Enrollment is defined in terms of the show rate which is the number of students who have applied and been accepted to a program. Enrollment increased from 97 in the fall or 2017 to 152 in the fall of 2018 for a 56% increase in enrollment. Additionally, there was an increase in the number students who receive Federal funding for education in the form of a Pell Grant.

Table 2: Cybersecurity Program Enrollment Data

	Students	Average GPA	% on Pell Grant
Fall 2017	97	2.72	20%
Fall 2018	152	2.94	60%

Table 3 displays transfer-in data at the college, program, and subject level. The transfer in rate is defined as students entering a program by transferring in. Rates at the college and program level have remained consistent.

Table 3: Transfer In Rate

	FA16	FA17	FA18
Overall CSCC	18.6%	19.2%	16.1%
CSCC Computer Science	27.9%	27.1%	21.8%
Cybersecurity	*	27.9%	15.0%

**Data not available*

Table 4 displays transfer out data at the college, subject and program level. Rates at the college and program level have remained consistent. The transfer out rate is defined as students exiting a program by transferring

out. Overall, transfer out rates have slightly increased over time at the college while there is not yet data available for the Cybersecurity program due to the fact that this is a new program.

Table 4: Transfer Out Rate

	FA16	FA17	FA18
Overall CSCC	26.2%	28.7%	30.4%
CSCC Computer Science	9.8%	12.0%	19.4%
Cybersecurity	*	*	*

**Data not available*

Table 5 displays GPA data at the college, subject and program level. GPA has remained mostly consistent over time but have steadily increased. Cybersecurity students had a higher average GPA as compared to all of CSCC and Computer Science students only.

Table 5: GPA

	FA16	FA17	FA18
Overall CSCC	2.72	2.75	2.81
CSCC Computer Science	2.66	2.72	2.82
Cybersecurity	*	2.97	2.89

**Data not available*

Table 6 displays graduation rates at the college, subject, and program level. Because the Cybersecurity program has a program cycle of two years, three-year graduation rates are displayed. This is in alignment with the way graduation rates are calculated among two-year institutions according to the National Center for Education Statistics. While Computer Science majors had similar graduation rates to that of all of CSCC, rates are not yet available for the Cybersecurity program.

Table 6: Three-year Graduation Rates

	FA16	FA17	FA18
Overall CSCC	6.6%	6.4%	8.3%
CSCC Computer Science	3.9%	7.4%	12.5%
Cybersecurity	*	*	*

**Data not available*

Student Exit Survey

Students exiting the Cybersecurity program were asked to complete a student exit survey the results are presented below.

Students were asked to rate their level of agreement with statements related to their educational experience as a student in the Cybersecurity program. Ratings were on a 4-point scale where 1 = strongly disagree and 4 = strongly agree.

Table 7: Educational Experience

	n	Mean (SD)
Communicate effectively	7	2.86 (.38)
Organize information	8	2.87 (.35)
Lead others	5	3.40 (.55)
Critically analyze information	8	3.00 (.54)
Develop global perspective	6	3.17 (.75)
Work in teams	7	3.57 (.54)
Understand the central concepts of my discipline	8	3.25 (.71)
Engage in ongoing professional learning	8	2.88 (.64)

Students were asked to rate their level of agreement with statements related to their educational experience as a student in the Cybersecurity program. Ratings were on a 4-point scale where 1 = strongly disagree and 4 = strongly agree.

Table 8: Overall Satisfaction

	n	Mean (SD)
Availability of faculty	8	3.13 (.64)
Course availability	7	2.14 (.90)
Class size	8	3.13 (.35)
Academic advising	8	3.25 (.71)
Library resources	7	3.00 (1.15)
Technological environment and resources	8	2.75 (.89)
Program instruction	8	3.38 (.74)
General education instruction	6	3.00 (.01)
Laboratory facilities and equipment	8	2.88 (.99)

Students were asked to rate their level of agreement with statements related to the degree to which their various components of their education would lead to employment. Ratings were on a 4-point scale where 1 = strongly disagree and 4 = strongly agree.

Table 8: Preparation for Employment

	n	Mean (SD)
Course Work	4	3.00 (.54)

Research Projects	4	3.00 (.63)
Capstone	3	3.00 (--)
Internship	4	4.00 (--)
On/off campus professional development	4	3.00 (.82)

Students were asked to rate their level of agreement with statements related to the rigor of the curriculum. Ratings were on a 4-point scale where 1 = strongly disagree and 4 = strongly agree.

Table 9: Challenging Curriculum

	n	Mean (SD)
The curriculum was challenging	4	2.63 (.74)
The curriculum provided a solid foundation for a job in cyber security	3	2.692 (.52)

Students were asked to rate their level of agreement with statements related to perceived value of their education. Ratings were on a 4-point scale where 1 = strongly disagree and 4 = strongly agree.

Table 10: Value of Education

	n	Mean (SD)
Rate the value of your education	8	3.38 (.74)
Rate the effectiveness	8	3.25 (.71)

Students were asked to report what their primary activity would be after graduation. The results are presented in Table 11.

Table 11: After Graduation

	% (n)
Full-Time Employment	83% (5)
Graduate or Professional School (Part Time)	16% (1)

Faculty Group Interview

Cybersecurity faculty who played a role in curriculum development were interviewed to get a sense of how curriculum and other program elements were developed and how the program can endure beyond the scope

of the current grant cycle. The results are presented below. A total of such faculty participated in group interviews conducted at the conclusion of the project. Results are presented below.

Q: When the cybersecurity curriculum was being developed, what gaps were discovered in the existing curriculum in terms of cybersecurity competencies & knowledge?

Table 12: Current Gaps

Theme	Frequency (%)	Definition	Comments
Career Ready Students	4 (23%)	The gap of not having qualified workers available for the workforce.	• Currently, in the central Ohio area and nationwide, roughly one out of three available cyber jobs remain vacant. The problem has become one of getting enough of the right education/training accomplished in a very compact period. • That talk about the open head count and the number of skilled professionals to fill them and that indicated a clear need nation-wide but also Ohio was one with a great need. • you know there was work done to address some of those areas that were emerging technologies or thoughts and make sure students were better prepared.
No Gaps	3 (29%)	There were no gaps in the existing curriculum.	• In fact, we set a goal to be in alignment with NIST standards and were just designated a Community of Academic Excellence in Cyber Defense for two years schools in March of 2019. This validates the robustness of our curriculum from an NSA/NIST standards standpoint and • The curriculum is very technically strong and quite aggressive and ambitious for the first two years of college…. • Accordingly, the Plan of Study is aggressive due to the desire to produce cyber educated individuals who can compete for available cyber jobs that require a very high degree of technical competency and experience.

Meeting Accreditation Requirements	2 (13%)	The gap of not yet meeting standards needed for accreditation	• By the time I was appointed as the PI on the grant in June of 2017, the cybersecurity curriculum was already identified and starting the process to make its way through the Ohio Department of Higher Education and the Higher Learning Commission in order to be accredited. • from a 'gaps' standpoint, we are attempting to balance what foundational requirements are needed for cybersecurity professional in the rapidly expanding and changing world of cyber security.
Strengthening Curriculum	2 (12%)	No major gaps were found, but small curriculum changes were made to strengthen the program.	• …I did not see any gigantic gaps but there were certainly tweaks made to the program to kind of enhance it. • We are looking to strengthen the following, without sacrificing too much of what we currently have in the degree…Cloud based cybersecurity – possibly focusing on CompTIA's Cloud+…More robust Secure Shell training
Lack of Program Support	1 (14%)	The gap of not having enough support when developing the program.	• I found myself in the position of not being able to both support the existing Network Security based Plan of Study and the badly needed Cybersecurity Plan of Study simultaneously…

Q: How were those gaps filled to ensure students would have the desired knowledge and competencies? If possible, please describe specific curriculum changes.

Table 13: Filling Gaps with Curriculum Changes

Theme	Frequency (%)	Definition	Comments
General Curriculum Changes	7 (61%)	Gaps were filled by making general curriculum changes to ensure knowledge and competencies.	• At the time we had to eliminate available credit hours from 73 to 65 in order to meet new state maximum guidelines. • as far as costs to the students. I am in the process with the OER folks creating OER content for the 2258 access course, just because the book that was originally proposed for that class that doesn't quite fit as nicely as I wanted it too, so I was in the

			process to get that OER set up and hopefully in the fall of 2020 that would be ready to go • The changed curriculum was already addressing gaps from the previous Network Security curriculum.
Course Specific Changes	3 (31%)	Gaps were filled by changing the courses available to ensure knowledge and competencies.	• We removed: BMGT 2250 Project Management Principles, ECON 2200 Principles of Microeconomics, CSCI 1145 HTML… • Changed to in order to meet a Cybersecurity orientation: PHIL 1150 Introduction to Logic to … CSCI 1103 Intro to Logic & Object-Oriented Programming… • Added: ITST 1101 Industrial Applications and Software (CompTIA IT Fundamentals+ Cert related)…

Q: Please describe challenges you faced in developing program curriculum.

Table 14: Challenges in Program Development

Theme	Sub-Theme	Frequency (%)	Definition	Comments
Acquiring Staff		7 (89%)	Not having staff to develop program curriculum was a challenge.	• That is an ironic fact of life with the things cause it's the exact problem that we are trying to solve. The problem with not having the workforce, and then not having the workforce to teach the workforce.

	Competitive Pay	2 (49%)	Being able to competitively pay staff was a challenge.	• Both time and trained cyber professionals that can teach are at a premium. Our ability to pay cyber professionals a commensurate salary to the profession itself is a challenge which is not surprising due to industries' need for those individuals in the private sector and their ability to pay them accordingly. • also we got a third full-time position open, so just finding folks that are qualified to teach for the salary that we offer them is a huge challenge. I am thoroughly thankful that we have the great adjuncts helping us out here, but from a full-time perspective we are definitely struggling to find qualified candidates to fill positions that are open.
	Content Creation Skills	2 (26%)	Not having staff to create content was a challenge.	• Just, getting content created has been a challenge. We have had some definite challenges with 2258 and the state that it was in. • The primary issue we have faced in developing program curriculum is the need for full time instructors to develop the new curriculum at the same time as fulfilling grant requirements and teaching a growing number of classes.

Q: Can you discuss any successful strategies in developing cybersecurity curriculum?

Table 15: Successful Strategies

Theme	Frequency (%)	Definition	Comments

Certification Focused Curriculum	1 (53%)	Focusing the curriculum on certifications would be a successful strategy.	• The move to provide as many cert related courses as possible has made it easiest to incorporate textbooks that have preparation for successful passing of the cert in mind. Since the Cert itself is already focused on the practical application of fundamentals for the cert concerned there is very good alignment for the curriculum. Additionally, the assumption of the goal to gain the NSA's CAE-CD credential ensured that we align to NIST standards, which both industry and the Federal Government respect. Our students are focused in the direction of the prevailing requirements for cyber professionals.
Better Pay for Instructors	1 (33%)	Being able to pay instructors better would be a successful strategy.	• None that I am aware of, I obviously. We have, it would be great if we could pay people more since they are in such demand, but you know the whole, I've only been at the college for over a year so, I don't want to misspeak but I know there is, the rate you pay an English teacher is the same rate you pay a cybersecurity instructor so there is not a whole lot deviation there.

Q: Beyond the scope of the current grant, how can the Cybersecurity program be sustained?

Table 16: Sustaining Program

Theme	Frequency (%)	Definition	Comments

Curriculum Changes	2 (52%)	The program can be sustained through small continuous changes to the curriculum.	• Were just continuing to identify gaps and fill those gaps as we can. After this grant is over, we will just continue to work with the local cybersecurity professionals, and you know stay up to date on things that are relevant. I would love to see some blue team red team activities… • I have planned to pitch the concept of working between the ethical hacking students and on the non-security side of things, the web map development, some of those classes and maybe team teaching a section where we do a, we have the students from the web app class develop web apps and the students from the pentest class , pentest the web apps and then provide feedback to the other students about the security of the applications they are developing. I don't know how difficult that coordination would be but that is something that I would bring up during our next meeting.
Acquiring Professional Staff	2 (9%)	The program can be sustained from hiring and retaining staff.	• Being able to track that permanent staff is going to be key here. That is the key challenge, I do not have a great suggestion on how to do that. • Can you discuss any successful strategies in developing cybersecurity curriculum?
Career Focus for Students	2 (7%)	The program can be sustained by focusing on getting students into careers.	• Creation of a flow of paying cyber students • THE CAE-CD designation and engaging our local industry partners in internships, work-study and apprenticeship programs will lead to jobs for students.

Industry Feedback on Graduates	1 (24%)	The program can be sustained through evaluating graduates with feedback from the industry.	• We had some panels people from the industry were brought in to discuss what they were seeing from graduates and let us know what they would like to see from folks coming out of the program. I think continuing to do that, bring people in from the industry, not necessarily teaching currently just people who are hiring our graduates and understanding what they are looking for. Maybe what they see as potential gaps…

Q: What changes would you like to see implemented in the program over the next three years?

Table 17: Changes

Theme	Frequency (%)	Definition	Comments
Curriculum Changes	3 (75%)	Changes to the curriculum should be made in the next three years.	• Yes. I would like to see a tighter linkage to the course work and the certification test. Like the final exam would be the actual certification exam, that would be awesome… • Mentioned earlier in my class we actually use one of the certification focused books as the course book and that kind of keeps things a little closer aligned. And also since those certifications were so popular the course books are actually much less expensive than some of the others… • Teaching all curriculum with increasing excellence. Adding/adapting cloud-based cybersecurity principles to the curriculum. Trimming down some overlaps in the curriculum to the minimum necessary. Leveraging Ohio's newly developing Cyber Range Capacities for hands on student experience
Increased Program Involvement	1 (7%)	Changes to the amount of student involvement should be made in the next three years.	• Developing Columbus State student participation in Cyber exercises and competitions. Development of a Columbus State Cyber Club

Industry Participation in Program	1 (6%)	Changes to the amount of industry participation should be made in the next three years.	• Continuing and expanded cooperation with industry, particularly as it relates to equipping Columbus State students
Acquiring Professional Staff	1 (2%)	Changes to the amount of staffing should be made in the next three years.	• The addition of one new full-time staff member.