PENINSULA COLLEGE

CYBERSECURITY & COMPUTER FORENSICS

Program Review

February 2, 2021

TABLE OF CONTENTS

CYBERSECURITY & COMPUTER FORENSICS

Program Overview

There are two parts to program review

1. Program viability
2. Program learning outcomes assessment

The Cybersecurity & Computer Forensics (CSIA) program prepares students for information security analyst and computer forensic careers. Foundation courses introduce students to the legal, ethical, and theoretical issues in cybersecurity and computer forensics technology. Core courses expand student depth and skills in ethical hacking, criminal justice, evidentiary analysis, and the development of a forensically sound environment. Capstone courses provide practicum experience and opportunity to test and troubleshoot computer security systems.

Degrees & Certificates

Degrees and certificates can be completed entirely online

- Cybersecurity and Computer Forensics AAS
- Cybersecurity and Computer Forensics AAS-T
- Computer Forensics Short Term Certificate of Completion
- Information Technology Systems Administrator AAS
- Information Technology Systems Administrator AAS-T

Enrollment and Student Achievement

	2016-17	2017-18
Enrollments	145	143
Class Success Rates (2.0 or above)	85%	85%
Retention-Fall to Fall	69%	91%
Completion-Degree/Certificate Attainment	62%	83%

Review of CSIA student enrollment, retention, and completion trends show improvement overtime. Improvements in enrollment are likely due to efforts, college wide, to improve outreach and engagement with prospective students including rapid hand-off from initial contact to program coordinator outreach as soon as student services notifies us of a new prospective student. Retention and completion improvements are influenced by focusing on student success through the following: 1) Listening to students and inviting them to share direct feedback 2) Willingness to try out new ideas and

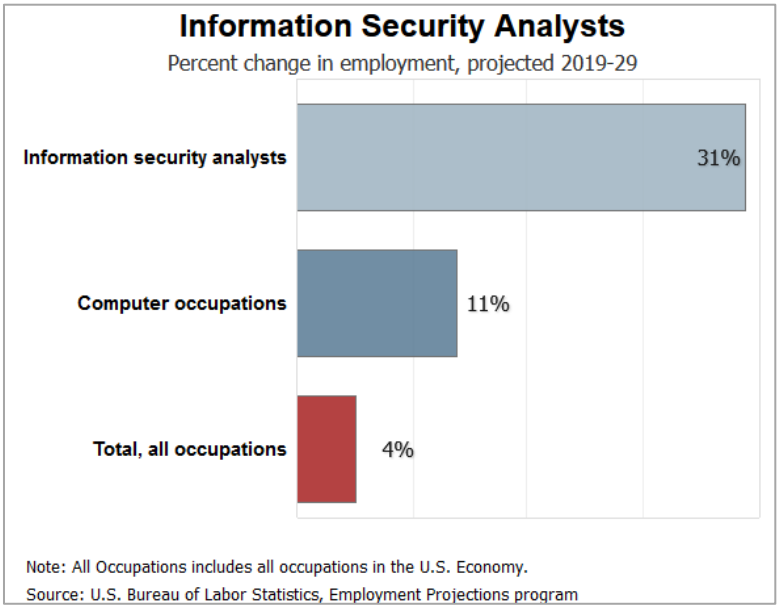
implement new instructional ideas based on student feedback and best practices 3) Taking great care in working with each student on advising and registration 4) Making improvements and measuring efficacy through the SLO and course/program review process. Disaggregated class pass rates show positive trends for most groups. Class pass rates for Native American/Alaska Native students is low. In response to this trend, we are in the initial steps of applying for a National Science Foundation (NSF) Advanced Technology Education Program grant. Our proposed project will expand and revise Cybersecurity and Information Technology courses to include culturally responsive curriculum that aligns with Native led industries.

Staffing

The CSIA program is currently offered online and staffed with one full-time and one-part time faculty member. The expanded use of virtual labs has reduced program infrastructure and equipment costs. When Cybersecurity classes are offered on-campus, program costs increase for computer equipment and information technology support services.

Workforce Trends

CSIA jobs in Washington State are in demand with an average annual growth of 2.5% by 2028 and average hourly wage of $57.38. Potential positions include Information Security Analyst, Information Technology Security Professional, Cybersecurity Specialist, Systems Engineer, Cybersecurity Engineer and Computer Forensic Analyst. The Bureau of Labor Statistics (BLS) projects Cybersecurity jobs will increase by 31% by 2029, much faster than average growth rate.



Active Advisory Committee

The CSIA program has an active and engaged advisory committee. Members include representatives from 7 Cedars Casino, City of Port Angeles, Clallam County PUD, First Federal Savings & Loan, Olympic Medical Center, Port Angeles School District, and US Coast Guard.

Accreditation Requirement

The CSIA program was developed in accordance with criteria from the National Centers of Academic Excellence for Information Assurance Education and Training Program for 2 Year Institutions (CAE-2Y). Course outcomes include skills standards set forth by the National Training Standard for Information Systems Security Officers (CNSSI No. 4014).

Articulations and Pathways

The CSIA program has current dual credit articulations with the North Olympic Peninsula Skills Center and Sequim High School. The CSIA AAS-T degree is articulated with Western Washington University's Bachelor of Computer and Information Systems Security. Graduates of the program may go on to pursue the Peninsula College BAS degree.

Program Currency

In its sixth year, the CSIA program continues to innovate and adapt to the dynamic landscape of the information system security field. Program technology is current and supports teaching, learning, and assessment of program and course learning outcomes.

Assessment and Improvement Planning

Cybersecurity assessment and improvement planning are documented in Course SLO Reports, Curriculum map, and biennial academic unit program review (AUPR).

Course SLO Reports

Review of the Cybersecurity course SLO reports show they are current and document continuous improvement planning. For example, the course SLO report for CSIA 190 include the following improvements.

1. Update knowledge, skills, and abilities to better align with CompTIA Security+ certification.
2. Assign lab worksheets to help student reflect what they learned in the lab.
3. Add review of concepts across multiple lab assignments to help student retain and apply new learning.
4. Expand labs into a quarter-long project in which the student builds their own virtual network environment rather than using one that has built for them.

Curriculum Map

The Cybersecurity curriculum map is current and documents where students achieve program outcomes within individual classes.

CURRICULUM MAP																	
Curriculum Maps represent where students are given the opportunity to achieve the outcomes, from introduction to mastery, as they proceed through the curriculum.																	
Program/Area of Study:																	
Degree/Cert: Cybersecurity AAS																	
Reporting Year: 2021																	
Program Learning Outcomes: Program outcomes should be measurable and specify what the student is expected to know upon completion of the program. Outcomes should be detailed, meaningful enough to guide program improvement, teaching and learning.	Course Numbers/Program Requirements: Type one of the following outcome categories for each class and outcome. **I= Outcome Introduced (I)**: Students are introduced to the idea, concept or skills related to the outcome at the general or basic level. **R= Outcome Reinforced (R)**: Students learn additional information related to the outcome. They may synthesize ideas or demonstrate a skill at a novice or intermediate level. **M= Outcome Mastery (M)**: Students are required to demonstrate their ability to perform the outcome with a reasonably high level of independence and proficiency.																
List Program Learning Outcomes Below. List course ID in the dark gray cells on the right (example ENGL&101, MEDIA 110)	CSIA 110	CSC 100	AMATH 121	IT 107	CSIA 185	CSIA280	IT 114	CSIA 190	SOCSCI 101	CSIA 195	IT 225	ENGL& 101	PSYC& 100	CSIA 290	CI 121	MEDIA 206	AOS 107
Demonstrate an understanding of the core concepts, tools, and methods used to secure computer systems. (CT)	I	I		R	R		R	R			R			M		R	
Identify and present indicators that a cybersecurity incident has occurred. (CT)	I			R		R		R			R			M		R	
Apply criminal justice methods to cybersecurity and computer forensic investigations.(I)	I													M	M		
Plan, implement, and evaluate penetration testing and ethical hacking of computer systems. (CT)	I									R				M			
Identify, analyze, and mitigate threats to internal computer systems. (CT)	I			R	R			R			R			M		R	
Collect, process, analyze, and present computer forensic evidence.(C)	I					R						R		M			R
Work in teams to analyze and resolve cybersecurity issues. (PI)	I													M			R
Apply critical thinking skills to risk analysis of computer systems.(CT)	I	I	R		R				R				R	M			

Cybersecurity & Computer Forensics Academic Unit Program Review (AUPR)

The 2018-2020 CSIA AUPR is complete and documents several improvements and results from SLO assessment.

Area of Study and/or Program Outcomes (Fill in this box with a program or area of study outcome)	**Method of Assessment & Planned Criteria** (How will you assess the outcome and what will success look like?)	**Improvements** (What improvements will you make to meet the planned criteria)	**Results** (Tableau data and/or results from Course SLO Reports)	**Analysis/Narrative of Results** (Use results from Course SLO Reports)	**Improvement Plan** (Use results from Course SLO Reports)	**New Funding**
Demonstrate an understanding of the core concepts, tools, and methods used to secure computer systems	Class success rates of 2.0 or above- aggregate all CSIA classes and Media 206.	Implement flipped classroom model in CSIA 110 and CSIA 195 incorporating video content from Lynda.com.	Success rates went from 85% to 89% between 2017-2018 and 2018-2019	CSIA 110 had a 20% increase CSIA 195 had a 13% increase in completion. The flipped classroom and Lynda.com changes positively impacted completion in these courses.	Add Lynda.com video resources and flipped classroom model for CSIA 185 and CSIA 190 courses.	No new funding needed.
Identify and present indicators that a cybersecurity incident has occurred	3.0 or higher on Assignment 11 - Forensics Capstone in CSIA 280. 3.0 or higher on phase 3 of CSIA 290 capstone project.	Add assessment to CSIA 280 and CSIA 290 to assess student's ability to determine when and if an intrusion has occurred.	All students who attempted the CSIA 280 forensics capstone (12 out of 19 students) assessment in Winter of 2019 achieved > 3.0. Have not yet completed phase 3 of this year's CSIA 290 capstone course.	12 out of 19 students in CSIA 280 Winter of 2019 achieved > 3.0 on the forensics capstone assessment.	Continue to develop and test the assessment of incident detection and response in CSIA 290 capstone course and monitor progress. We will be adding an additional incident detection/response assessment in the CSIA 280 forensics course in Winter 2020 as well.	No new funding needed.
Apply criminal justice methods to cybersecurity and computer forensic investigations	3.0 or higher on CSIA 280 Module 1 quiz, Module 3 quiz and Module 4 quiz.	Add case studies for chain of custody examples in CSIA 280.	CSIA 280 scores from Winter 2019: 96% average score on Module 1 Quiz, 94% average score on Module 3 Quiz and a 96% average score on the Module 4 Quiz.	The current assessment method for this outcome is being exceeded.	Continue to monitor the three key assessments for this outcome while adding chain of custody case studies in Winter 2020.	No new funding needed.

CYBERSECURITY & COMPUTER FORENSICS

Area of Study and/or Program Outcomes (Fill in this box with a program or area of study outcome)	**Method of Assessment & Planned Criteria** (How will you assess the outcome and what will success look like?)	**Improvements** (What improvements will you make to meet the planned criteria)	**Results** (Tableau data and/or results from Course SLO Reports)	**Analysis/Narrative of Results** (Use results from Course SLO Reports)	**Improvement Plan** (Use results from Course SLO Reports)	**New Funding**
Plan, implement, and evaluate penetration testing and ethical hacking of computer systems	Class success rates of 2.0 or above CSIA 195	Develop penetration testing planning project for CSIA 195.	Success rates went from 87% to 100% between 2017-2018 and 2018-2019	CSIA 195 had a 13% increase in completion.	Penetration testing project has been a beneficial addition to the course. We will continue with the project and compare results next year.	No new funding needed.
Identify, analyze, and mitigate threats to internal computer systems	Class success rates of 2.0 or above in CSIA 110	Add vulnerability analysis project to CSIA 110	Success rates went from 74% to 94% between 2017-2018 and 2018-2019	Added the vulnerability analysis project in Fall of 2019 and success rates are now at 94%.	Will continue to make the vulnerability analysis project a key component in CSIA 110 and will monitor progress.	No new funding needed.
Collect, process, analyze, and present computer forensic evidence	3.0 or higher on CSIA 280 Module 4 quiz.	Implement final forensic investigation project and assessment in CSIA 280	96% average score on the Module 4 Quiz.	Students are doing well on the current assessment method.	Continue monitoring performance on CSIA 280 module 4 quiz. Implementing a final forensic investigation project in CSIA 280 this quarter (Winter2020).	No new funding needed.
Work in teams to analyze and resolve cybersecurity issues	3.0 or higher on CSIA 290 capstone project.	Add a minimum of one additional team-based project to at least two courses (CSIA 195 and CSIA 110)	No data available yet as the CSIA 290 capstone course offered winter.Will publish results in next year's AUPR.	Quarter long, team project added to CSIA 110 and CSIA 195 in fall of 2019. Capstone course hasn't yet completed so no data available yet.	Monitor, collect feedback, and modify team projects for CSIA 110 and CSIA 195 going forward. Publish results of capstone course to AUPR.	No new funding needed.
Apply critical thinking skills to risk analysis of computer systems	Class average grade of 2.0 or above in CSIA 110 and CSIA 185	Develop risk analysis project for CSIA 290 capstone course.	Class average for grades in CSIA 110 and CSIA 185 are > 2.0.	Currently, the class average for grades is above the 2.0 benchmark.	Implementing a CSIA 290 risk analysis project in the current instance of the course (Winter 2020) with NICE Challenge.	No new funding needed.

CYBERSECURITY & COMPUTER FORENSICS

Area of Study and/or Program Outcomes (Fill in this box with a program or area of study outcome)	**Method of Assessment & Planned Criteria** (How will you assess the outcome and what will success look like?)	**Improvements** (What improvements will you make to meet the planned criteria)	**Results** (Tableau data and/or results from Course SLO Reports)	**Analysis/Narrative of Results** (Use results from Course SLO Reports)	**Improvement Plan** (Use results from Course SLO Reports)	**New Funding**
Quantitative Reasoning: Apply basic computational skills to practical applications	Class success rates of 2.0 or above- aggregate all CSIA classes and Media 206.	Identify courses in the program where additional quantitative reasoning-based projects and assessments can be added.	2018-2019 academic year: Class average for all CSIA courses and MEDIA 206 were > 3.0	Class average grades are high so we will continue to make sure the new, additional challenges, projects and assessments continue to help students be successful while challenging them.	Add better instruction and tools for base ten to binary to hexadecimal number systems to CSC 100	No new funding needed.
Communicate in writing for a variety of purposes and audiences	Class success rates of 2.0 or above- aggregate all CSIA classes and Media 206.	Implement assessment rubrics for written assessments in at least two courses (CSC 100 and CSIA 110).	Rubrics were developed and implemented in CSC 100 and CSIA 110.	Addition of rubrics in CSIA 110 and CSC 100 in fall of 2020 made feedback and grading significantly more efficient.	Continue adding rubrics to two more CSIA courses. CSIA 195 and CSIA 280 courses will be next.	No new funding needed.
Demonstrate competencies to succeed in the selected career pathway workplace	1) Students will participate in a volunteer or service-learning opportunity. Criteria for assessing is feedback/report from workplace supervisors. 2) Mock interviews	1) Identify new volunteer and service-learning opportunities for students to participate in actual workplace projects. 2) Develop a mock interview program for capstone class	1) Due to the pandemic new opportunities were limited. 2)Mock interviews will be added to the spring 2021 capstone class	CSIA 195 students completed a project for a local organization in fall 2020 for (P.A.S.D). Mock interviews will continue to be part of CSIA 290. Added in Winter 2020 so no data yet.	CSIA 195 students completed a project for a local organization in fall 2020 for (P.A.S.D). Mock interviews will continue to be part of CSIA 290.	No new funding needed.

Conclusion

This program review demonstrates the Cybersecurity faculty actively assess SLOs and implement improvements that support student success and academic excellence. The program is in-demand with high potential for exponential job growth over the next 8 years. The program focuses on student success and workforce development for the college's service area and beyond. Labor market data and community input provide evidence that the program is popular with employers and students. Program level assessment showed a need to improve the way online lab activities were delivered to students across the college's large two county service district. To address this challenge, faculty added virtual labs and new assessment rubrics to assess student performance from a distance. In hindsight, early adoption of virtual labs allowed Cybersecurity faculty and students to learn remotely with little to no interruptions from the pandemic.