The Synergy of Intertwining Grant Activities: Cyber Up! and GenCyber Girls

Abstract

The ongoing workforce shortage of skilled and diverse cybersecurity professionals coupled with the continued upward trend of cybercrime has led to an increased number of funding opportunities from the federal government to support projects focused on technical skills development. Significant emphasis is placed on academic transfer pathways and education-to-career pathways for students from K-12 to community college and beyond. Utilizing funding from multiple sources, faculty have intertwined grant project activities to increase awareness of cybersecurity careers and academic pathways, emphasizing digital forensics and incident response. The two grant projects, Cyber Up! and GenCyber Girls, aimed to develop college-level curriculum and cybersecurity workshops for female high school students. Project activities were synthesized to create a summer camp for high school students based on the curriculum developed for the college programs in digital forensics and incident response. The synergy between the projects has shown an increase in female participation in the digital forensics course and helped build interest in cybersecurity careers among K-12 students.

1. Introduction

According to recent projections, by 2025, the cost of cybercrime will increase to $10.5 trillion globally [1]. Additionally, impacts on emotional and mental health are among the many untold costs of cyberviolence, which range from online sexual exploitation and threats of violence to cyberstalking, bullying, and harassment [2] [3]. Ransomware attacks that cease operations and seize data are of particular concern because of the potential for loss of life at scales both small and large when the attack targets are hospitals, 911 operations, and healthcare providers. Public alert bulletins expressing particular concern and precautions for ransomware attacks were posted by the Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) to help raise awareness about this looming cyber threat to various agencies [4].

In a 2020 post, officials from Microsoft reported that the sophistication of cybercriminals has increased with top attacks focusing on stealing credentials and ransomware [5]. The attacks are relentless, conducted by skilled attackers, and continuously changing or morphing to avoid detection. The dominant attack types have shifted over recent years from malware, such as viruses, worms, and spyware, to phishing in which email is used to mimic well-known brands in an attempt to harvest usernames, passwords, and other sensitive personal information from individual consumers and employees. These tactics can be easier to disseminate widely with a broader impact. While there is essentially no global legal authority to stop malware distributors and prevent sales of stolen data and offensive attack tools available on the dark web, the rise in cybercrime is expected to continue [6].

Threat actors are not required to be credentialed and only have to get the attack mechanism right one time to penetrate an organization's defenses, while security professionals defending an organization must get it right 100% of the time to prevent major data breaches or network attacks from being successful. Considering all of this, the cybersecurity community is at a disadvantage with the workforce shortage of talented cybersecurity professionals affecting organizations'

ability to address their cybersecurity needs. Women in cybersecurity are significantly outnumbered by their male counterparts, which brings about a compelling need to increase the number of individuals interested in learning about cybersecurity to decrease the gender gap and diversify the cybersecurity workforce [7] [8] [9]. Curriculum in specialized cybersecurity education programs such as digital forensics and incident response is also not standardized or widely available.

By offering cutting-edge, online cybersecurity education, Coastline Community College (Coastline) is uniquely positioned to aid in developing a diverse and competitive cybersecurity workforce, namely through its national position in cybersecurity education and its standing in the online education community. Coastline has leveraged two grant projects to simultaneously develop new curriculum for an associate degree in digital forensics and incident program while also developing a pipeline of interest in the program through outreach events at the middle school and high school levels.

2. Coastline College's cybersecurity program

Coastline College's Cybersecurity program is focused on the mission-critical issue of building a skilled and diverse workforce of individuals that are prepared for cybersecurity and law enforcement careers. Coastline College (Coastline) is an associate degree-awarding institution located in Orange County, California, leading the state in the proportionality of online enrollment (Coastline 58%, State 25%). Coastline serves a diverse student population, which extends beyond the College's service area; over 60% of Coastline's students reside outside of district boundaries. The College has programs that position it to serve underrepresented minorities, first-generation college students, and special populations (e.g., disabled students, foster youth, economically disadvantaged).

Coastline is a National Center of Academic Excellence in Cybersecurity (NCAE-C), first designated in 2014 by the National Security Agency (NSA) and Department of Homeland Security (DHS). Typically, between 850-1,000 students enroll in Coastline's cybersecurity and computer networking programs each year with a broad distribution of races and cultures, self-identified as Asian, Hispanic, and White. Coastline's dedication to building the cybersecurity workforce is reflected in the pathways of five degrees and 12 certificates offered. The content for these courses is aligned with the NCAE-C Community's knowledge units derived from the work roles of the NICE Cybersecurity Workforce Framework [10].

Over the years, the College has been awarded several grant-funded project opportunities, including one to help establish relationships among community colleges and universities as the Southwest Regional Hub, another to develop a federally registered cybersecurity apprenticeship program, to develop cybersecurity curriculum, and others to increase cybersecurity career awareness among middle school and high school teachers and students. The focus of this paper is on two projects funded by the National Science Foundation (NSF) and the NSA's GenCyber program. First is the Cyber Up! Digital Forensics and Incident Response project (Cyber Up!) (Award #1800999), which was awarded to Coastline by the NSF's Advanced Technological Education (ATE) program, which focuses on two-year institutions of higher education with support for curriculum development, professional skills development, and development of career

pathway [11]. The overarching purpose of the Cyber Up! award is to develop cybersecurity curriculum that will be made available to the public to adapt and adopt.

Second is Coastline's GenCyber Girls award from the NSA started in March 2020 with the summer 2020 camp delayed due to the stay-at-home and social distancing orders during the COVID-19 pandemic (Award #H982302010075). The girls camp was hosted on-site at Coastline's Garden Grove campus in August 2021, with pre-camp activities in July and concluding with post-camp activities in January 2022. Promotions were directed towards female students of diverse backgrounds to assist in diversifying the future cybersecurity workforce.

The emphasis on cybersecurity skills and digital forensics careers in both projects presented an opportunity to intertwine the grant activities of Cyber Up! and GenCyber Girls, leveraging many of the professional relationships previously established for the Cyber Up! project to develop a camp for high school students that would act as a pathway for the Digital Forensics and Incident Response (DFIR) program at Coastline. Building early awareness of Coastline's cybersecurity and DFIR programs with high school students increases opportunities for faculty to engage with students during the selection period while post-secondary education options are considered [12].

3. Cyber Up! Digital Forensics and Incident Response project

The three-year performance period for the Cyber Up! project award began in October 2018. The project is now in its fourth year after a no-cost extension was approved to complete project activities by September 2022. Activities for the project are in the final stages, with four of the courses already having been offered on Coastline's general fund schedule. The two remaining courses are in the final stages of development, with lab assignment development in progress. Final versions of the six courses will be complete by the end of the extended performance period.

Cyber Up! is designed to provide remote learning opportunities and remote lab activities for students to learn tools, techniques, and procedures used in industry. Faculty from Coastline College and Fullerton College collaborated with industry and government professionals to develop six program courses in cybercrime, digital forensics, and incident response, helping to prepare students with hands-on technical skills and knowledge for the workforce. The distance education modalities of Coastline's Cybersecurity and DFIR programs are designed for a national reach and assist in preparing students for successful employment and financial independence.

3.1. Goals of the Cyber Up! project

The primary purpose of the Cyber Up! project was to develop six courses in Digital Forensics and Incident Response leading to a two-year Associate of Science (AS) degree and Certificate of Achievement to be offered at Coastline College. To accomplish this, the team set out to research other similar projects and programs to adapt and adopt from their models, research industry and government needs to find relevant cybersecurity workforce frameworks and industry-recognized certifications and assemble an advisory board of subject matter experts currently working in government, industry, and academia to provide input and guidance based on expertise.

Using these combined resources, course outlines for a series of six courses in digital forensics and incident response were developed. Table 1 below shows the course numbers, titles, and

number of units for the six courses. An AS degree and a Certificate of Achievement in Digital Forensics and Incident Response were created from the series of courses. Model course content and hands-on lab assignments for four of the six courses have been arranged in the online platform that Coastline College uses Canvas Learning Management System. The project team has continued disseminating project updates to the advisory board and the broader cybersecurity community via email, meetings, professional social media (LinkedIn.com), the ATE microsite (https://ate.is/cyberup/), papers, and conference exhibits and presentations.

Table 1. Certificate of Achievement in Digital Forensics & Incident Response

Course Number	Course Name	Units
CYBR C150	Intro to Digital Forensics	3
CYBR C160	Intro to Incident Response	3
CYBR C170	Cybercrime and CSIRT Coordination	3
CYBR C250	Intermediate Digital Forensics	3
CYBR C260	Intermediate Incident Response	3
CYBR C280	Advanced DFIR Capstone	3
	Total	18

The project has picked up momentum since late 2020 when a lack of resources for lab development caused some delays in progress. The first four courses have been offered, which has provided for student feedback and assessment of learning outcomes. The final steps will be to finalize course content for all six courses and then to disseminate model course content to other interested colleges and universities to adapt and adopt for their institutions.

3.2. Approach to curriculum development

An initial review of other similar academic programs was conducted to include the AAS in Cyber Forensics from Union County College in Cranford, New Jersey, the Bachelor of Science in Computer Forensics and Digital Investigations from Champlain College in Burlington, Vermont, and the Advanced Technical Certificate in Cybersecurity and Cyberforensics from Daytona State College in Daytona Beach, Florida. From this and other resources, a framework of six college-credit courses was developed. The project intended to develop curriculum and course content by incorporating widely recognized workforce development resources, including CyberSeek, SANS, and the NICE Cybersecurity Workforce Framework [13] [14] [10].

Figure 1. Cybersecurity Workforce Development Resources

The Cyber Up! team assembled an advisory board of experienced industry professionals, government, and cybersecurity faculty from two-year and four-year institutions. The first meeting was used to share an overview of the project goals, the purpose of advisory board involvement, and introductions of the newly assembled advisory board members. Using a synthesis of the top skills requested for the work roles of Cyber Crime Analyst / Investigator and Incident Responder Analyst from CyberSeek, the SANS Institute DFIR exam objectives for Certified Forensic Examiner and Certified Incident Handler, along with the NICE Workforce Framework knowledge, skills, and abilities, baselines for discussion with the advisory board were established [15]. It was also noted that the materials developed should be community college-level appropriate.

The drafts for six course outlines were created based on the synthesized content above. During the follow-up meeting with the advisory board, each course was reviewed to observe any gaps or missing topics from an industry perspective, and the board members' feedback was collected on course topics and hands-on lab tools and objectives. Nearly all advisory board members were in attendance to gather synchronous feedback, and two met with the project team separately to provide additional time for a deeper analysis and overall feedback. The meeting served several outcomes to improve course outlines, develop course and lab objectives, and refine student learning outcomes.

Faculty reviewed the workload of each course to define the scope and ensure a balance between course materials and hands-on lab assignments based on the number of lecture, lab, and contact hours for a three-unit course. The proper curriculum process for the Career Education division was followed, starting with a labor market data request from Los Angeles and Orange County Regional Consortium (LAOCRC), then submission for local approval from Coastline College's Curriculum Committee, a request for approval from the Board of Trustees at Coast Community College District, regional consortium approval from LAOCRC, and finalized by state approval from the California Community College Chancellor's Office.

3.3. Long-term significance of the Cyber Up! project

An external evaluator aided in the short-term quantitative review of the academic programs created by the project team. To date, four of the six DFIR courses have been offered publicly. These courses were used in the annual formal assessment and evaluation of the program by the external evaluator. A qualitative review of the grant project activities was also reported.

In the third annual report, the evaluator noted strong leadership, major goal achievement, strong outreach and recruitment efforts by the project team, strong program enrollment in the face of declining College enrollment, indications of deepening industry partnerships, and signs of early adopters of the DFIR program at other higher education institutions. Key performance indicators (KPI's) for the project included the establishment of the DFIR associate degree and certificate, course participation demographics, program enrollments including retention and success, industry partnerships, replication by adopters, and articulation agreements. For comparison purposes, the population demographics for Orange County, CA have been included side-by-side with the course participation demographics for academic years 2019-2020 and 2020-2021.

Table 2. Course Participation Demographics

Ethnicity, Gender, and Socio-Economic Status (Introduction to Digital Forensics)	2019-2020	2020-2021	Orange County Population
Total Student Enrollment/Population	49	54	3.18M
White	35%	20%	40%
Hispanic/Latinx	47%	30%	34%
Asian	14%	30%	21%
Black or African American	4%	9%	2%
Female	14%	26%	51%
Economically Disadvantaged	33%	42%	11%

The project team has developed new and significant relationships with college faculty, universities, government agencies, industry professionals, K-12 teachers, and Career and Technical Education Counselors. These partnerships increase communication, improve collaboration, and lead to more successful outcomes on other projects. Student skill development and course completion will continue to be a significant part of the DFIR program as industry needs continuously change, and students' prior computer experience will differ over time. Coastline faculty anticipate an expansion of the DFIR program to increase elective course offerings of specialized courses such as mobile forensics and cloud forensics in the next couple of years.

4. GenCyber Girls project

The GenCyber Program Office is located at the National Security Agency, with the aim to increase cybersecurity awareness, prepare teachers for cybersecurity curriculum, and increase student diversity at the K-12 level through summer camps and year-round workshops hosted by colleges and universities across the country [16].

The initial agenda for Coastline's GenCyber Girls Camp was developed by Coastline faculty in collaboration with FBI special agents to create hands-on activities for high school girls that focused on careers in digital forensics and law enforcement, with meditation twice a day for stress relief. The GenCyber camp workshops focused on law enforcement roles with an *Intro to Quantico* theme as the girls experienced a mock investigation using the techniques learned at camp. Workshop presenters included government agents, college faculty, high school teachers, and industry professionals to provide campers with broad knowledge of career pathways and job expectations. At the summer camp, law enforcement professionals discussed careers and scenarios encountered in fieldwork, demonstrating just how vital this work is to our Nation's security.

4.1. Goals of the GenCyber Girls project

Increasing awareness of cybersecurity issues and careers through hands-on activities to engage 40 female students at the high school level was the goal of the GenCyber Girls project at Coastline College. Coastline hosted a one-week summer camp in 2021 that introduced 37 high school students (36 female and one male) to the types of activities conducted by professionals working in digital forensics based on an FBI Intro to Quantico theme. The curriculum for the workshops is developed by the camp staff comprised of college faculty, high school, and middle school teachers to ensure that age-appropriate material is designed for the campers. The middle school teacher provides the expertise in engagement methods and educational technology tools to maintain the campers' interest.

Ancillary benefits included relationships established with local FBI representatives, local middle school and high school teachers, industry professionals working in technology roles, and high technology professional organizations. New ideas and opportunities have emerged from these relationships as well.

4.2. GenCyber Girls camp and workshop events

Prior to the on-campus workshops, virtual meetings provided an overview of cybersecurity concepts, ethics, online safety, and a professional speakers panel. At Coastline's GenCyber Girls camp, students examined digital evidence using industry tools to locate suspicious activity related to the purchase of tiger cubs in a mock case. In teams, the campers developed a forensic report which included their examination of the digital evidence, their findings of suspicious activity, and how the evidence was case related. On the last day of camp, the student teams presented an overview of their forensics examination and analysis to FBI agents, industry professionals, and college faculty.

Camp activities included a realistic forensics investigation, multiple presentations and interactions with FBI agents, a mock crime scene for the chain of custody workshop, a tour of the FBI's mobile forensics van, a presentation by Fontana Police Department's K-9 unit, and concluded by student team presentations to demonstrate the skills and knowledge gained throughout the camp. On the final day of camp, a ceremony was held to recognize the extra efforts and skills of the campers. Multiple awards were presented, including team awards for the highest score in the capture-the-flag competition, best forensics report, and best findings in the forensic report. Two individual awards were presented, the first was for Most Inquisitive during

the investigation, and the second was for Most Career Oriented. All camp attendees were presented with an individual certificate of participation, recognizing their contributions and efforts throughout the week.

After the GenCyber Girls camp, additional workshops were hosted at Coastline's campus and at South Lake Middle School in December and January. GenCyber camp attendees were given priority registration to the December workshop to allow teams to reconnect and share updates since the camp. As a result of the camp survey feedback, these events focused on introductory coding and cybersecurity careers.

Along the pathway, CyberTech Girls no-cost annual workshops at Coastline include an introduction to cybersecurity careers, academic pathways, hands-on hardware, mock crime scene with forensics case analysis, and many other specialty activities. Role models from industry and government provide attendees with diverse perspectives about different work roles and pathways. Other opportunities include the annual CyberTech Expo which is open to the community and the CyberPatriot monthly training and competition open to middle school and high school students in Coastline's service area. This variety of activities provides young women with the awareness of online safety and sparks their interest in education pathways to cybersecurity careers.

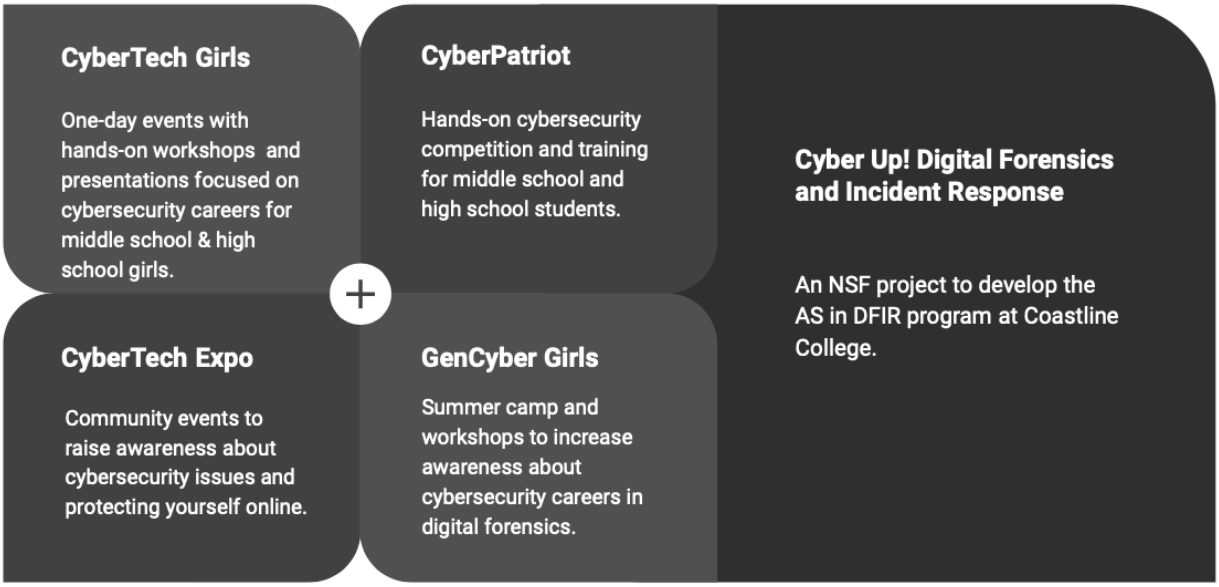

Figure 2. Cybersecurity Pathways

Activities such as these help increase skills and cybersecurity knowledge in diverse and underrepresented populations help to assure increased participation of women, minorities, and special populations in science, technology, engineering, and mathematics (STEM) education and in the technology workforce. Coastline's cybersecurity program strives to generate essential new knowledge and skills to share with students, professionals, and the academic community.

4.3. Survey

Camp staff surveyed campers daily to ensure camp activities were on track and again at the end of camp to gather comments and feedback for future activities. Daily surveys asked campers about their interest in the activities and learning opportunities. Campers consistently showed interest in the content each day. At the end of the camp, most campers expressed interest in continuing their studies in cybersecurity. Some said they planned to start a club on campus in the fall; some said they had a high interest in pursuing a career in digital forensics or cybersecurity, and others asked about returning for more events. A couple campers asked about returning as a mentor for others because they had extensive experience with CyberPatriot competitions and programming that they thought would benefit incoming campers.

Many of the girls were very enthusiastic about cybersecurity careers at the end of the camp. The camp significantly contributed to the goal of GenCyber by helping to inspire students to create clubs, play cyber competitions, and share their interest in cybersecurity with others. The follow-up activities are expected to reinforce campers' ongoing interest in cybersecurity.

An external site visit was conducted mid-week, and the observations noted that during whole-group instruction, team activities, and individual activities, the campers were highly engaged.

Commendations from the strengths section of the external evaluation report included:

> "This was a model student camp."
>
> "The partnership with the FBI was cutting edge and focused on digital forensics and a link to cybersecurity careers for women."
>
> "Diversity based on socio-economic status, ethnicity, experience, and gender supported GenCyber's goals of reaching underserved populations."

Of the 37 campers, 31 submitted responses to the end-of-week survey from GenCyber's external evaluation team. The responses were split up to form three categories of incoming and outgoing interest levels for comparison: low, moderate, and high. The bar chart shows a substantial increase in outgoing interest for the low incoming interest group, increasing from 12.67% to 68.59%. A moderate increase for the moderate incoming interest group, increasing from 52.12% to 71.75%. There was a slight decrease for the high incoming interest group, down from 75.75% to 75.36%.

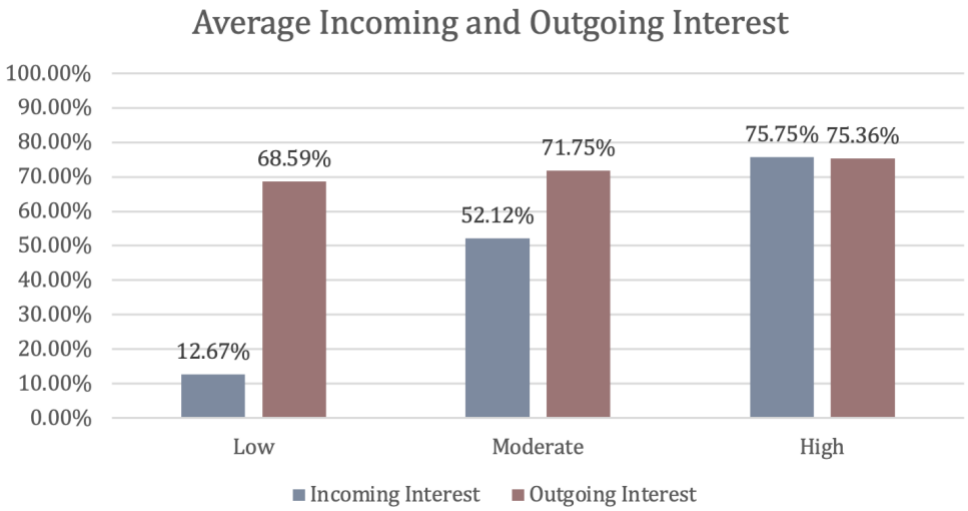

Figure 3. Average Incoming and Outgoing Interest. GenCyber Evaluation Report. August 2021.

Qualitative feedback was also grouped using these three categories. Interestingly, some of the same items that were described as interest development enablers for some were also described as decreasing interest for others. Comments about things that happened at camp which enabled interest in cybersecurity were the mock investigation, finding evidence in the case, using digital forensics software, meeting guest speakers, and the mobile forensics van. Comments about things that happened at camp that decreased interest included difficulty using the new software, long work time, the activities, a camper came with the expectation of coding, and some activities felt like time-fillers.

5. Synergy of intertwining grant activities to develop cybersecurity pathways and the talent pipeline

Protecting our Nation's critical infrastructure and the information of individual citizens requires cyber resilience and a skilled cybersecurity workforce made up of diverse individuals. Project team members leveraged the synergy between the goals of the two projects for Cyber Up! and GenCyber Girls to increase awareness of digital forensics careers, including law enforcement roles. Through the college curriculum, labs, and faculty resources, the team provided extensive training during the GenCyber Girls summer camp.

Hands-on training exercises in digital forensics evidence analysis techniques were developed for the GenCyber Girls camp using the forensic images created for the Cyber Up! project. Focusing on the topics of the Introduction to Digital Forensics course, short training activities were designed for the high school students to learn about evidence collection and analysis procedures using OS Forensics and ProDiscover software. Campers worked in teams of four throughout the week to walk through the software and catalog evidence to develop their report based on the scenario given at the start of camp.

6. Inhibitors and delays

The California statewide decline in enrollment for two-year higher education has dampened the previously expected increase in interest in the DFIR program [17]. An assumption could be made that the suspension of student loan payments, increase in federal and state stimulus checks, and the stay-at-home orders have changed the landscape of education with a shift in individual priorities and the lack of availability to add coursework to already overloaded work-life activities [18] [19] [20]. Other implications such as the College's reduced overall marketing funds may also play a key role in the inability to increase the number of students enrolled in the DFIR program.

The increased volume of remote work impacted the availability of experienced cybersecurity professionals to collaborate on the Cyber Up! project for the lab development portion [21]. Considerable technical skills and understanding of academic coursework were needed to develop labs that meet the requirements of the course and fit the intended skill level of students. The delay has a bright side which is the opportunity to offer more of the DFIR courses prior to the end of the grant performance period, which was originally requested by the NSF Program Office before the award was issued.

7. Short-term outcomes

Recent outcomes are abundant, starting with the establishment of a team of experienced professionals with common goals to develop the talent pipeline and increase diversity in the cybersecurity workforce. One of the additions to the team retired from law enforcement and took on a new role as part-time faculty teaching digital forensics. The new curriculum offerings for college credit in the asynchronous online learning format are already being offered at Coastline, and one student reported a new job in law enforcement after taking just one class, Introduction to Digital Forensics.

A collection of hands-on lab assignments and virtual machines has been created with expertise from professionals that have worked in the field, providing students with engaging activities that help them develop the skills needed for in-demand jobs in digital forensics and incident response. The labs can be used for workshops and activities outside the classroom because they have evidence depth and multiple real-world scenarios to draw from.

All of the workshops, activities, and community events work to increase cybersecurity awareness locally within the Orange County region amongst middle school, high school, and college students, which in turn will increase diversity in the cybersecurity workforce of the future. Another positive outcome of the GenCyber camp was one of the attendees was nominated by the Program Director and then honored by the National Center for Women and Information Technology (NCWIT) with the Aspirations in Computing award in February 2022.

The proportion of female students in Coastline's cybersecurity program has notably increased from 16% in 2015-2016 to 22% in 2020-2021. Faculty strive to help change the landscape in the cybersecurity workforce by offering outreach activities that address gender gaps and underrepresented populations, deficiencies in cybersecurity career awareness, and lack of

exposure to technical content. Through these experiences, the faculty have received additional opportunities to work with very experienced faculty at other institutions across the country.

8. Long-term potential

As evidenced by the increase in female participants in the Introduction to Digital Forensics and the GenCyber Girls survey results, the DFIR program and academic pathways have the potential to contribute to the goals of the NSF ATE and GenCyber Program Office. Digital forensics skills are increasingly in demand and the number of positions requiring technical knowledge is expected to continue to rise over the coming years [22] [23] [24]. This could contribute to increased enrollment in the program.

Plans for the next academic year include regional collaboration on digital forensics workshops for first responders in law enforcement roles. This effort will bring together faculty and experienced professionals for mutual benefit to gain valuable feedback on the material and provide free training to professionals for immediate use on the job.

Faculty use continuous improvement processes such as annual and comprehensive program reviews and student learning outcome assessments to ensure that the course content will be updated, evolving to meet industry demands and cybersecurity needs as they change over time. Sharing course outlines and labs with other higher education institutions across the country allows for collaboration and exchange of ideas to promote continued updates. The curriculum modules will also be available to other institutions using curriculum repositories such as the Canvas Community environment, the CAE resource directory known as CARD, and CLARK Center.

9. Conclusion

For many, the ongoing need to develop the talent pipeline for a diverse cybersecurity workforce of the future is compelling. Curriculum development, pathways and educational program road mapping, outreach events, and cybersecurity awareness activities are anticipated to be part of the solution to developing cyber resilient organizations that can withstand the increased volume of cyberattacks to come. Young women deserve the opportunity to experience hands-on cybersecurity activities and learn about cybersecurity careers early on to choose post-secondary education that can lead to high-wage, in-demand careers.

GenCyber and NSF ATE funding provides opportunities for young women, underserved and underrepresented populations, K-12 teachers, and higher education faculty through synergistic projects that are both creative and strategic. Being involved in the GenCyber and ATE communities since 2018 has been rewarding and energizing due to the notable upward trend in female enrollment in the Cybersecurity program at Coastline College. The program will continue to evolve and mature to keep up with rapidly advancing technology with the intent to provide in-demand, online education for diverse student populations working towards the successful attainment of degrees and certificates.

References

[1] S. Morgan, "Cybercrime to cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, 13 November 2020.

[2] "2020 Internet crime report," Federal Bureau of Investigation, U.S. Government Printing Office, 2021.

[3] J. Hawdon, "Cybercrime: Victimization, Perpetration, and Techniques," American Journal of Criminal Justice, no. 46, p. 837–842, 2021.

[4] "Ransomware Activity Targeting the Healthcare and Public Health Sector, Alert (AA20-302A)," Cybersecurity and Critical Infrastructure Agency, 2020. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa20-302a.

[5] T. Burt, "Microsoft Digital Defense Report," Microsoft, 2020.

[6] T. Stevens, "Cyberweapons: power and the governance of the invisible," International Politics, vol. 5, no. 3-4, p. 482–502, 2018.

[7] L. Amo, "Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy," IEEE Security & Privacy, vol. 14, no. 1, pp. 72-75, 2016.

[8] S. Furnell, "The cybersecurity workforce and skills," Computers & Security, vol. 100, 2021.

[9] C. Radu and N. Smaili, "Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure," Journal of business ethics, 2021.

[10] "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: https://www.cisa.gov/nice-cybersecurity-workforce-framework.

[11] "Advanced Technological Education (ATE)," National Science Foundation (NSF), 2022. [Online]. Available: https://beta.nsf.gov/funding/opportunities/advanced-technological-education-ate.

[12] T. Vaarmets, "Gender, academic abilities and postsecondary educational choices," Journal of Applied Research in Higher Education, vol. 10, no. 3, p. 2018.

[13] "Hack the gap," CyberSeek, 2022. [Online]. Available: https://www.cyberseek.org.

[14] "About," SANS Institute, 2022. [Online]. Available: https://www.sans.org/about/ .

[15] "Cyber Security Courses and Certifications. Digital Forensics and Incident Response.," SANS Institute, 2022. [Online]. Available: https://www.sans.org/cyber-security-courses/?focus-area=digital-forensics .

[16] T. Ladabouche and S. LaFountain, "GenCyber: Inspiring the Next Generation of Cyber Stars," IEEE security & privacy, vol. 14, no. 5, pp. 84-86, 2016.

[17] W. Jay-Jr, E. Ramos, S. Quinonez and L. Hudson, "Research shows that community colleges across Calif. see overall enrollment decline paired with incline in Distance Education enrollment," University Wire, 2021.

[18] N. Gullett, M. Haddad and L. Hatch, "To Pay or Not to Pay: Student Loans and the CARES Act," Journal of Financial Planning, vol. 34, no. 8, pp. 66-72, 2021.

[19] B. Cummings, "Stimulus Checks and Child Tax Credits and Taxes, Oh My!," Journal of Financial Planning, vol. 34, no. 10, p. 20, 2021.

[20] S. Wrycza and J. Maślankowski, "Social Media Users' Opinions on Remote Work during the COVID-19 Pandemic," Information Systems Management, vol. 37, no. 4, pp. 288-297, 2020.

[21] E. Şentürk, E. Sağaltıcı, B. Geniş and Ö. Günday Toker, "Predictors of depression, anxiety and stress among remote workers during the COVID-19 pandemic," Work, vol. 70, no. 1, pp. 41-51, 2021.

[22] "Forensic Science Technicians," Bureau of Labor Statistics, Occupational Outlook Handbook, 18 January 2022. [Online]. Available: https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm.

[23] E. Torpey, "Careers in forensics: Analysis, evidence, and law," 2009. [Online]. Available: https://www.bls.gov/careeroutlook/2009/spring/art02.pdf. [Accessed 2022].

[24] "Computer and Information Technology Occupations," Bureau of Labor Statistics, Occupational Outlook Handbook, 8 September 2021. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/home.htm. [Accessed 2022].