ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Creating a Repeatable Nontechnical Skills Curriculum for the University of Southern Maine (USM) Cybersecurity Ambassador Program (CAP)

Lori L. Sussman | Department of Technology, University of Southern Maine, USA, ORCID: 0000-0003-3667-0340
Zachary S. Leavitt | Department of Technology, University of Southern Maine, USA, ORCID: 0000-0003-3667-0340

Abstract

The workforce demand for skilled cybersecurity talent has exceeded its supply for years. Historically, the pedagogical approach was to identify and create curricula for the most in-demand technical knowledge, skills, and abilities (KSAs). Unfortunately, the field has tended to neglect nontechnical counterparts. However, recent literature suggests a core set of nontechnical KSAs that employers seek after. This study explored the codification of a nontechnical curriculum for a cybersecurity internship program at the University of Southern Maine (USM). The USM faculty created the Cybersecurity Ambassador Program that can serve students and the community. The service to students is to make them more attractive to employers. The benefit to the community is to provide cybersecurity awareness training to vulnerable populations. This discussion about the USM CAP serves as a case study for other programs considering this type of enrichment using an internship model. CAP started as an informal program, but this research used objective data to create repeatable blueprints. The researchers designed these lesson plans to help students progress from novices to competent in crucial nontechnical skills delineated in the National Initiative for Cybersecurity Education (NICE) Workforce framework. The team used a mixed methods approach to baseline

Received: 23.05.2023

Accepted: 19.09.2023

Published: 19.09.2023

Cite this article as:
L.L. Sussman, Z.S.Leavitt "Creating a Repeatable Nontechnical Skills Curriculum for the University of Southern Maine (USM) Cybersecurity Ambassador Program (CAP)," AICG, vol. 2, no. 1, 2023,
DOI: 10.60097/ACIG/162858

Corresponding author:
Lori L. Sussman,
Department of Technology,
University of South Maine,
USA, ORCID:
0000-0003-3667-0340;
E-MAIL:
lori.sussman@maine.edu

Tier 1/novice students' skill levels, place them in a cybersecurity enrichment program, track their progress, and determine program efficacy in helping them achieve beginner status. The information shared can serve as a point of departure for a case study that might guide other programs interested in doing similar work.

Keywords

NICE Workforce Framework, cybersecurity education, cybersecurity training, cybersecurity ambassador, cybersecurity internships

1. Introduction

IN 2013, like many highly connected nations, the United Kingdom (UK) looked deeply into its cybercrime reports to find actionable trends. Researchers were astonished that network and computer hygiene could prevent 80% of cyberattacks [1, p. 4]. However, the report also found that the workforce needed to be more robust to answer individual and organizational needs. A lack of science and technology courses in UK schools created a workforce gap that would take decades to fill [1, p. 27]. This demand for cybersecurity (CS) talent is not limited to the United Kingdom. In the United States (US), the Cybersecurity and Infrastructure Security Agency (CISA) created the National Initiative for Cybersecurity Careers and Studies (NICCS) to address teacher and student skill shortages. Unfortunately, while these national initiatives helped universities target essential CS knowledge, skill, and abilities (KSAS), they lacked blueprints to create student programs [2]. The hard work of developing repeatable and scalable programs fell on academia to create programs that meet workforce needs.

1.1. Mining for New Talent Pools

The current cybersecurity workforce must be improved to satisfy the demand for qualified cybersecurity professionals. Experts predict this shortfall will continue for several years [3]. As recently as 2018, researchers found that an excess of 1.5 million positions will be unfilled in the global cybersecurity workforce. Businesses seek employees with technical and interdisciplinary credentials to help fill this cybersecurity gap [4]. Given the shortage of qualified cybersecurity professionals, new talent pools of applicants are needed.

Cybersecurity employers historically have overlooked women and people of colour to fill essential roles [5]. In 2021, women comprised more than 50% of the US population, yet, only 35.5% majored in science, technology, engineering, and mathematics (STEM) disciplines [5]. In addition, the US has a large minority population that is increasing over time but does not enjoy representative numbers in the computing sciences. [6]. Women and minorities can fill this CS workforce gap and should, as they have a vested interest. In 2014, data revealed that a million more US women than men had their identities stolen [7]. On average, people of colour, African American, and people of Latino descent are two to three times more likely than white people to become victims of fraud related to debt or income [8].

Moreover, existing security technologies disadvantage women and people of colour. For example, biometric facial recognition systems have trouble identifying the faces of women and people of colour [9]. Therefore, increasing women and minorities in cybersecurity enlarges the talent pool and provides new perspectives to improve technologies and practices within the field.

1.2. Next Generation Cyber Professional Curriculum Development

Hiring managers created job descriptions that screen potential employees for cybersecurity skills in various tools and systems. As such, candidates who made it to the interview stage often had comparable technical skill sets. However, it was often nontechnical, called soft skills, that got the candidate the job [10]. Industry, government, and academia members noted that CS graduates frequently lacked the necessary soft, hard, and mixed nontechnical KSAs for employment [11]. Employers almost universally recognize that entry-level workers need client-facing KSAs to accomplish the organization's cybersecurity goals. KSAs involving written and oral communication, teamwork, problem-solving, and critical thinking skills were particularly important [10, 11].

The impetus for the Cybersecurity Ambassador Program (CAP) program started with University of Southern Maine (USM) cybersecurity students who wanted to do community outreach. The faculty worked with the State of Maine Office of Securities and the Maine Economic Initiative Fund (MEIF) to secure initial grant funding to make this community engagement program a paid departmental internship. As part of the grant requirements, the sponsor asked the faculty to create a program that served students and the community. There was also a requirement to research the efficacy of the approach. After securing approval from the USM Institutional Review Board (IRB), the faculty moved forward to create a model that could serve as a case study for other cybersecurity educational organizations.

The faculty recruited students and prioritized those who had Federal Work Study (FWS) funding and students who needed to take the mandatory internship class for their program of study. FWS students usually worked ten hours per week, and interns worked twenty hours per week during a sixteen-week semester. The 2019 cohort started with two students but was cut short due to COVID restrictions. The primary advisor had to recast the program as entirely virtual for the next three years. The program involved fourteen students in seven cohorts (Tab. 1).

Table 1. Student Participants.

Undergraduate Students in Cohorts	
Fall 2019	2
Fall 2020	2
Spring 2021	4
Fall 2021	5
Spring 2022	5
Fall 2022	7
Spring 2023	7
Graduate Assistants	
AY20-21	1
AY21-22	3
AY22-23	3

The emphasis on community service by providing cybersecurity awareness training to vulnerable populations is an ideal vehicle to focus on needed nontechnical KSA development. CAP promoted CS awareness and education through research and outreach opportunities that, in turn, required students to elevate communications and leadership skills. The program leveraged undergraduate and graduate students seeking to make meaningful contributions to local communities as the students gained vital professional competencies.

1.3. Skill Acquisition

Proficiency via objective assessment was critical. The program used stages from the Five-Stage Model of Adult Skill Acquisition as its conceptual model [12]. This framework describes how people learn skills and identifies five stages of progress novice, advanced beginner, competent, proficient, and expert. The faculty presumes students enter the program at the novice level, defined as the Bronze/Tier 1 stage. The blueprint for the program scaffolded instruction sequentially and progressively while allowing participant autonomy to consume the content. As Dreyfus noted, "The student needs not only the facts but also an understanding of the context in which that information makes sense" [12, p. 177]. The intention was to construct a professional development journey for these students to progress to advanced beginners, corresponding to the Silver/Tier 2 proficiency, a second sixteen-week program. This advanced beginner signpost stage, characterized by exposure to sufficient examples of meaningful activities, is critical for students' ability to apply learning to new and novel situations. When students achieve mastery of the silver curriculum, they have reached the competent stage, commemorated by promotion to Gold/Tier 3 status.

2. Methods

The researchers used a phenomenological study approach with structured and semi-structured data collection methods. Over sixteen weeks for this pilot, the researchers observed students, assessed their assignments, conducted interviews, and objectively evaluated participants performing various internship activities. The objective was to provide students with enhanced education, experience, and exposure to cybersecurity awareness and training research. The researchers used US Commerce's National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) – specific nontechnical KSAs in a focused way for curriculum development. The intention was to enhance 19 nontechnical skills from the NICE Workforce Framework using student-led projects for community awareness training. External assessment of the program was uniformly positive. For example, the National CyberWatch Centre identified this program as the 2021 Cybersecurity Curriculum Best Innovation. The faculty also received several other awards from the Epsilon Pi Tau (EPT), a technology honour society. The primary investigator won the EPT Warner award in 2021, 2022, and 2023 for presentations to the Cybersecurity Ambassadors. Student participants also received numerous internal USM recognition and received job offers at faster rates than nonparticipating students. As such, this program design can serve as a valuable case study for other academic institutions interested in similar student enrichment opportunities.

2.1. Program Design

The program used standard job site internships to provide opportunities for concurrent college credit. CAP created a cohort of student interns each academic semester who had demonstrated interest/ability in cybersecurity career pathways. The Principal Investigator (PI) created a three-tier program. The Cybersecurity Ambassador (CA) students achieved the first or bronze tier through oral and written assessments based on technical training and career planning modules developed and taught by working cybersecurity researchers and cybersecurity professionals. The second (silver) phase emphasized leadership and mentorship. The PI and Coordinator assessed student outreach leadership and peer training/mentorship, incorporating data into cybersecurity awareness and training research efforts. The top (gold) level was where students functioned at the programmatic level, helped coordinate outreach, and certified other students. These tiers correspond to novice, beginner, and advanced beginner levels of expertise.

The program gave participants paid entry-level cybersecurity internships, which allowed them to use the class for their program's mandatory internship requirement. The CAP created a cohort of student interns each academic semester who founds ways to learn nontechnical skill mastery as they pursued Cybersecurity career pathway material. The Principal Investigator (PR) intended to create a three-tier program to incentive continued participation and skill mastery. The Cybersecurity Ambassador (CA) students achieved the first or bronze tier through oral and written assessments based on technical training and career planning modules developed and taught by working Cybersecurity researchers and Cybersecurity professionals. The second (silver) phase emphasized leadership and mentorship. The PI and Coordinator assessed student outreach leadership, peer training/mentorship, incorporating data into cybersecurity awareness and training, and their research efforts. The top (gold) level was where students functioned at the programmatic level, helped coordinate outreach, and certified other students.

2.2. Nontechnical Skill Curriculum Development Process

The faculty advisor that founded CAP derived requisite nontechnical KSAs for cybersecurity students using those listed in the National Initiative for Cybersecurity Education (NICE) Workforce

Framework. Graduate Assistants used these KSAs to formulate learning objectives and activities for bronze-level students to access in their weekly skill enrichment modules in the university learning management system [10] (Tab. 2).

Table 2. These are the 19 NICE nontechnical competencies from the Workforce Framework. Graduate students and faculty create activities and assess mastery. Note students have three signpost stages. KSAs were scaffolded to be sequential and progressive.

KSA's	Curriculum Map
Presentation skills	Bronze (Tier 1)
Developing positive customer relations	Bronze (Tier 1)
Written communications skills	Bronze (Tier 1)
Working effectively with peers	Bronze (Tier 1)
Intellectual curiosity	Bronze (Tier 1)
Using computers effectively	Bronze (Tier 1)
Adaptability	Bronze (Tier 1)
Professional demeanour	Bronze (Tier 1)
Training	Bronze (Tier 1)
Ethics in decision making	Bronze (Tier 1)
Managing personal stress	Bronze (Tier 1)
Customer Service Problem Resolution	Silver (Tier 2)
Knowledge of core business processes	Silver (Tier 2)
Knowledge of and compliance with legal and regulatory requirements	Silver (Tier 2)
Managing crises	Silver (Tier 2)
Critically using information for decision making	Gold (Tier 3)
Facilitating teams and teamwork	Gold (Tier 3)
Negotiating techniques	Gold (Tier 3)
Leadership abilities	Gold (Tier 3)

Initially, observation was the predominant evaluation mechanism to assess student mastery. However, the need to codify the CAP curricula became apparent as the program grew. The team developed research approaches that supported the university's cybersecurity credentialing, provided a repeatable curriculum that students enjoyed, and met the goals of enriching skills that made participants particularly attractive workforce candidates. This vision spawned research questions that focused on nontechnical skill attainment for students with some STEM and cybersecurity background and included in the Bronze/Tier 1 curriculum:

1. How can the CAP objectively assess student baseline KSA of novice (Bronze/Tier 1) KSAs?
2. How can the team craft maximum flexibility into the Bronze/Tier 1 curriculum to accommodate different paces for participants?
3. How can the program objectively assess nontechnical KSA mastery progress from novice (Tier 1) to beginner (Tier 2)?

This rigor provided measurable data on students' progress and improved learning techniques.

The team created a 16-week curriculum designed to increase the speed of acquisition and retention of nontechnical KSAs by bronze-level ambassadors enrolled in the CAP. This research is a snapshot of the pilot group. The team received and filled out a baseline and a weekly survey to measure ambassadors' perceptions of their KSA development. The team also asked participants to suggest improvements to curriculum areas.

In this survey, the team asked the ambassadors to respond to each of the following three statements using a Likert scale from "strongly disagree" to "strongly agree":

- First, the content was relevant to the weekly learning objectives.
- The content was well-organized and easy to understand.
- Finally, the learning activities and assessments were effective in reinforcing the content.

Additionally, the team asked ambassadors to identify the best aspect and most challenging parts of each module. The survey incorporated a text area to capture feedback for these two questions and the question, "What is one thing we could do better for the next group?"

The feedback provided by the bronze-level ambassadors provides opportunities for future refinement and improvement of the curricula.

This qualitative data collection used a pre- and post-curriculum self-evaluation survey to measure ambassadors' perceptions. The objective was to capture the bronze-level ambassadors' journey from novice to advanced beginner. The survey instrument used a Likert scale to measure the ambassadors' confidence in their abilities associated with the targeted KSA.

The researchers also quantitatively measured proficiency via quizzes, discussion posts, and assignments graded by rubrics. These assessment techniques allowed for objectively validating mastery for KSAs at the novice level. Table 3 shows the mix of objective tools used.

Table 3. Objective Measures of KSA Proficiency.

Quiz	Handbook Knowledge
Quiz	Professional Demeanour
Quiz	Ethics in Cybersecurity
Graded Assignment	Article Review
Graded Assignment	Handout Creation
Graded Assignment	Presentation Deck Creation
Graded Assignment	Progress Reports
Graded Assignment	Discussion Posts
Graded Assignment	After Event Reflection

The researchers began the instruction process by decomposing the task environment into context-free features that the beginner could accomplish without the desired skill [12]. The learning management system (LMS) had posted rules for the Bronze Ambassadors, which allowed them to navigate the curriculum through self-paced modules. The students used their internship time to consume materials, complete assignments, and get feedback to improve results.

2.3. Assumptions, Limitations, and Scope

Several significant limitations impacted the design and outcomes of this study. The two biggest challenges were time and money. Academic semesters are typically sixteen weeks, but administrative items such as onboarding, vacation, and finals consume one to three weeks. Therefore, the designers had to condense the program to 13 – 14 weeks. Also, not all Ambassadors had the same number of hours each week. Because funding for CA pay came from both internship grants and the Federal Work-Study Program, half the Ambassadors worked ten and about half worked 20 hours per week. As such, the program had to have a flexible and achievable design to meet the program-related objectives.

The team balanced new content creation by incorporating pre-existing content for each curriculum module. Content specifically tailored for CAP use was ideal. However, creating content for each module described in the following section proved too expensive, time-consuming, or both. As such, the 16-week CAP curricula included newly built and previously published content. When possible, the team used free online e-learning platforms and tools like LinkedIn Learning or Coursera since they had built-in ways for students to prove their proficiency.

The team delivered the program entirely online, using Brightspace. Use of an LMS assisted in monitoring and assessing the effectiveness of the CAP curricula's objectives. The weekly curriculum survey also offered an opportunity to solicit any access issues. Additionally, CAs could raise concerns asynchronously via the CAP Discord tool.

The asynchronous delivery allowed students access to the course materials at their convenience. Supplemental material was available to CAs via Brightspace and a shared CAP Google Drive. The team also used external content from platforms such as YouTube, but the downside was that this approach relied on provider availability of the provider for access. The team created as much video content as feasible during this sixteen-week session.

The research team recorded all Brightspace data, including student progress and assessments, in a separate Google Drive accessible only to the research team. In addition to this data, the researcher also collected qualitative data from Qualtrics survey results. This survey captured participant self-evaluations. This multi-faceted approach to data collection allowed the team to understand the ambassadors' experiences with the curricula and evaluate the efficacy of the nontechnical KSAs developed through the program.

2.4. Participants/Sample

The team employed purposive sampling to select participants who met specific criteria. The initial sample consisted of four bronze-level CAs hired onto the spring 2023 CAP cohort. However, one participant withdrew from the program before its completion, leaving three participants for the study. The participants were undergraduate students who had not yet gained significant work experience in the CS field. They were selected based on their potential to develop the nontechnical KSAs identified in the study. Additionally, the participants represented historically underrepresented demographics in the CS and IT disciplines.

The three participants were diverse regarding their demographic backgrounds, including gender and ethnicity. All participants had completed introductory courses in their cybersecurity program and expressed interest in pursuing a career. The participants were highly motivated and committed to developing their skills in the CAP program.

Pilot participant demographics were relatively diverse. Of the ambassadors who completed the pre-survey, 75 percent identified as Caucasian, and the remaining 25 percent identified as Black. Data showed an even split between male and female participants. About half of the participants had earned a bachelor's or associate's degree, while the other half had some college education but no degree. It is worth noting that none of the cohorts had previous experience in the field of CS or had served in the US Armed Forces. As a result, the participants in this study represent a historically underrepresented group in the CS workforce and highlight the need to diversify the field.

2.5. Data Collection

The CAP used free software or software provided at no cost to students enrolled in the UMS. This software included programs from Brightspace Learning Management System (LMS), Microsoft 365 (Word, Excel, PowerPoint, etc.), Google Workspace (Gmail, Slides, Drive, etc.), and standalone programs like Canva, Discord, Trello, Zoom, and Zotero. The research team required the CAs to agree to the end-user license agreements (EULAS) and privacy policies of the software mentioned above. Researchers did not gather data from tool use. Instead, qualitative exploration using the web application Brightspace and a Qualtrics survey were collection tools.

Brightspace is USM's LMS and offers features to conduct online assessments, host discussion forums, and deliver remote instruction to students. Students were familiar with the tool before joining CAP–the study design generated data from participants' interactions with the content disseminated via Brightspace. Like the above software, students had to accept the EULA and data privacy policy for Brightspace before enrolling in USM's online courses. By extension, participants in the 16-week CAP curricula had to opt into the Brightspace privacy policy to participate in the study.

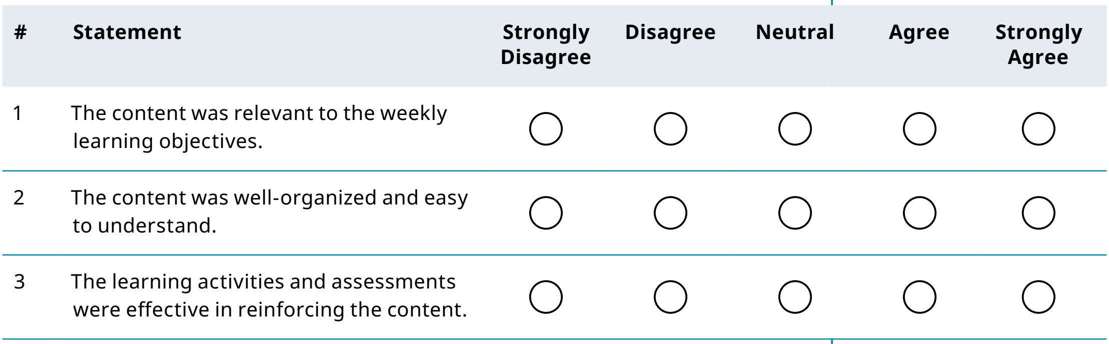
Instead of using personally identifiable information (PII) such as the ambassadors' first or last name or email address, the team coded and anonymized all student data. Researchers used randomly generated identification numbers for all participants. As with Brightspace, students who used Google Drive, Gmail, or Slides had to accept the privacy policies and any EULAs of that software before participating in the study.

3. Results

3.1 Qualitative Results

During the study, researchers discovered that not all participants provided feedback every week due to the modules' omission in weeks 10 through 15. This erratic feedback was a Brightspace survey limitation because the system mapped them in advance and did not update with an evolving curriculum. Additionally, the initial implementation of the survey radio option in Brightspace improperly grouped data. That idiosyncrasy affected the count of each value on any question using a Likert scale.

For instance, one of the survey questions asked participants to rate their agreement with the statement "The content was relevant to the weekly learning objectives" on a scale of 1 to 5, with one being strongly disagreed and five being strongly agreed. While the survey accurately captured participants' written responses, the data grouping was inaccurate, which could have impacted the analysis of the data (Fig. 1).



#	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	The content was relevant to the weekly learning objectives.	○	○	○	○	○
2	The content was well-organized and easy to understand.	○	○	○	○	○
3	The learning activities and assessments were effective in reinforcing the content.	○	○	○	○	○

Figure 1. Likert Scale Questions in the Brightspace Survey. It demonstrates a partial evaluation of the Brightspace curriculum modules. This figure is an April 1st, 2023 snapshot.

To address the data grouping issue, the team created individual surveys for each curriculum module and released them to participants who had not yet provided feedback for weeks 10 through 15. This approach allowed for the accurate capture of data related to each module. The team also created individual surveys for weeks one through eight but hid them from users to prevent data duplication and use in future semesters. Individual surveys for each module allowed for a more detailed analysis of the feedback received, which will inform the ongoing development of the CAP curriculum.

The purpose of this study was to evaluate the impact of a cybersecurity professional development curriculum on the skills and knowledge of participants. The pre-and post-curricula measured changes in confidence levels and understanding of various KSAs. The results of the pre-curricula survey indicate that participants generally had a moderate level of confidence in their presentation, written communication, negotiation, and crisis management abilities, with mean scores ranging from 3.25 to 4.5 out of 5. Participants also demonstrated a moderate understanding of cybersecurity compliance and legal and regulatory requirements, with a mean score of 3.25 out of 5. However, participants reported lower confidence levels in their ability to resolve cybersecurity problems and seek out cybersecurity news and information, with mean scores of 2.75 and 3 out of 5, respectively.

After completing the cybersecurity professional development curriculum, participants reported significant improvements in their confidence levels and understanding of various skills and knowledge domains (Fig. 2).

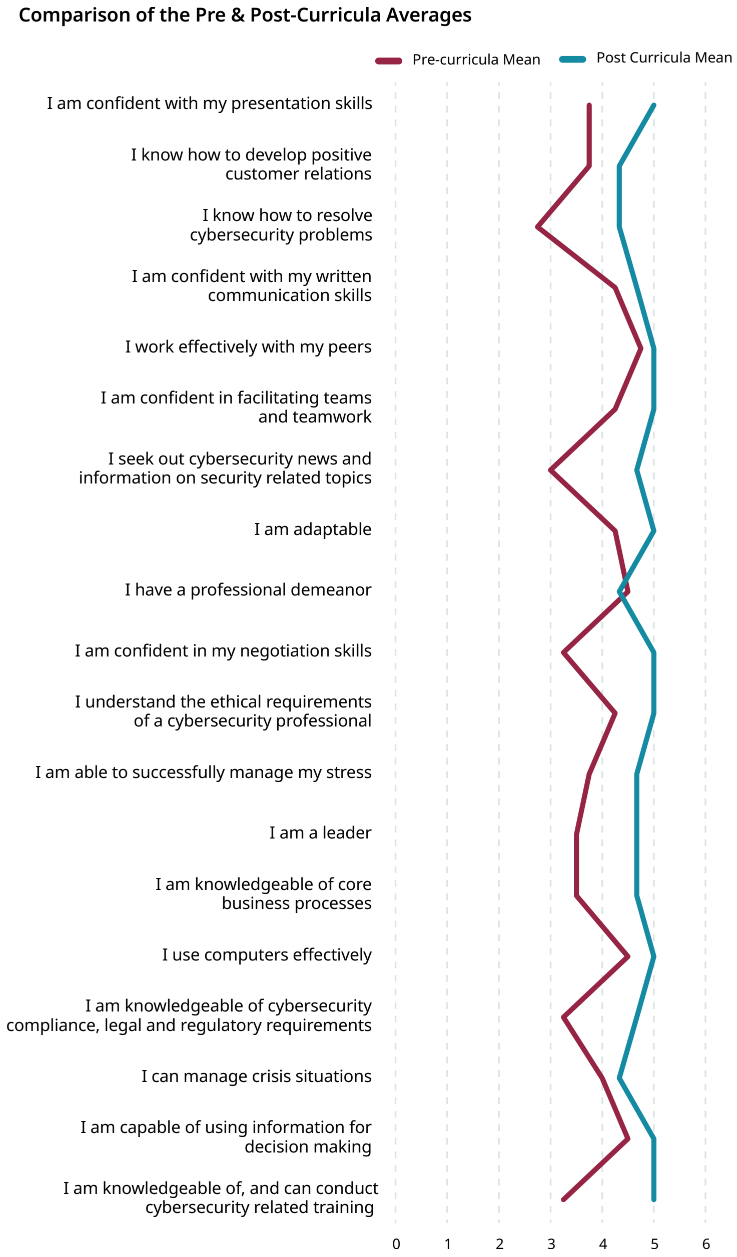


Figure 2. Comparison of the Pre- and Post-Curricula Averages. It depicts a comparison of the change of averages between the pre-and post-curricula KSA inventory surveys.

The post-curricula survey results show that participants' confidence levels increased significantly in all domains, with mean scores ranging from 4.33 to 5 out of 5. Participants also reported a substantially higher understanding of cybersecurity compliance and legal and regulatory requirements, with a mean score of 4.67 out of 5. Moreover, participants reported a significant improvement in their ability to resolve cybersecurity problems, seek out cybersecurity news and information, and effectively work with peers, with mean scores ranging from 4.33 to 5 out of 5 (Fig. 2).

3.2. Quantitative Results

The quiz design included a pool of questions and displayed ten randomly to the student. There was no time limit, but they only got one attempt. Assignments had a rubric to assure objective and consistent grading by faculty and graduate assistants, but the feedback was either “pass” or “redo” (Tab. 4).

Table 4. Pilot Results.

Assessment	Title	Student A	Student B	Student C
Quiz	Handbook Knowledge	97.23%	100.00%	97.23%
Quiz	Professional Demeanour	100.00%	80.00%	90.00%
Quiz	Ethics in Cybersecurity	60.00%	50.00%	50.00%
Graded Assignment	Article Review	Pass	Pass	Pass
Graded Assignment	Handout Creation	Pass	Pass	Pass
Graded Assignment	Presentation Deck Creation	Pass	Pass	Pass
Graded Assignment	Progress Reports	Pass	Pass	Pass
Graded Assignment	Discussion Posts	Pass	Pass	Pass
Graded Assignment	After Event Reflection	Pass	Pass	Pass

The students showed consistency of mastery of the handbook and professional demeanour content. However, there was consistent underperformance in the cybersecurity ethics topic.

4. Discussion

This study assessed the CAP curricula' effectiveness in developing targeted nontechnical KSAs among bronze-level ambassadors using qualitative and quantitatively collecting instruments. The team formulated three research questions to guide the study toward its intended purpose. First, the results indicated that the 16-week bronze-level CAP curricula enhanced participants' skills and knowledge in various domains. In addition, the significant improvements in their confidence levels and understanding of the topics indicated the move from novice to advanced beginner stages. Based on these findings, the data suggests that this program should continue to use this repeatable process and start working on the curriculum to help students move from beginner to advanced beginner signpost stages.

4.1. Qualitative Findings

The qualitative data indicated that the participants saw the opportunity to work on meaningful projects, have clear objectives for evaluation, and get practical experience as the most valuable aspect of the internship. The feedback from their self-assessments indicated increased confidence in all graded areas. The slight declination in professional demeanour may have been due to the combination of low objective quiz scores despite high pass rates on the assignments. Regardless, these students uniformly appreciated the chance to apply what they learned in the classroom to real-world situations and work alongside experienced industry professionals. To this point, one student said the following,

> *This experience has contributed to enhancing my professional attitude, and as a result, my self-perception has changed. I now have increased confidence in presenting in public and explaining cybersecurity terms to nontechnical individuals, which means I have gained confidence in my ability to communicate effectively with diverse audiences.*

The survey feedback indicated that this internship program provided an excellent work culture with sufficient supervision and feedback to grow. The qualitative data showed that CAP provided a supportive and inclusive work environment, and the curriculum helped gain future employment.

4.2. Quantitative Findings

There could be many reasons the students performed well in the first two quiz areas but not the third. It could be due to differences in interest, motivation, learning style, or prior knowledge. For example, Student A might have a strong interest in Handbook Knowledge and Professional Demeanour content and might have prior knowledge or experience in these areas. On the other hand, Student A might have less interest or prior knowledge of cybersecurity ethics.

The assessment may not be a good measure of student learning or mastery. For example, the evaluation might not align with the learning objectives or might not be measuring the right skills or knowledge. For this reason, the research team is reworking the ethics module and quiz questions.

Finally, the underperformance could explain why students self-reported less confidence in their professional demeanour at the end of the program. The researchers did categorize ethics as a subcategory for the students. They may have seen their lack of quantitative performance on the quiz as a reason to question their mastery of content in this area. The interviews indicate the plausibility of this explanation. The student feedback was that the experiences on the quiz and with different vulnerable populations made them self-aware that they had more to learn. The researchers discovered that they must make professional demeanour mastery at the novice, beginner, and advanced beginner levels clearer to students. In this case, they had novice mastery. Still, they expected a higher level of skills usually commensurate with Silver/Tier 2 level, thus reporting a decrease in anticipation of further skill mastery in this area.

4.3. Findings Based on Mixed Methods

The first research question explored the creation of an objective baseline instrument for participants. The one developed using the NICE Workforce Framework, and the Five-Stage Model of Adult Skill Acquisition provided an effective tool. The data from this survey showed that students self-identified as having a solid foundation in various CS KSAs, according to the comparison of the pre-and post-curricula surveys of bronze-level ambassadors enrolled in corresponding CAP curricula. The pre-curricula poll revealed that most students already felt confident and proficient in these subjects, with mean values above 3.5 for most skills. However, the post-curricula survey showed that the students' confidence and proficiency in some of these areas had increased even further, with mean values for several skills rising above 4.5.

The higher variability in some skills, such as leadership and core business processes, suggests that some students needed more practice in these areas. In addition, while the post-curricula survey showed an improvement in confidence and proficiency for these KSAs, their mean values remained below 4.5, indicating that there is still room for improvement.

The second question dealt with curriculum flexibility. The conceptual model allowed the team to develop questions to identify critical nontechnical KSAs that help ambassadors progress from novice to beginner and evolve the content accordingly. The data analysis shows that the CAP curricula design, which included written communication, customer service, and stress management, helped develop these critical skills despite students being at different skill levels and needing to absorb the content at different speeds. Students developed skills through lectures, reading, and hands-on activities. This experiential learning provided students with a comprehensive understanding of concepts and necessary nontechnical KSAs when they were most available to absorb the content.

The third research question explored objective measuring approaches for monitoring students' progress from novice to advanced beginner. The findings show that the 16-week CAP curricula used various assessment methods to measure student progress, including formative assessments, quizzes, and activities. These assessments helped to evaluate students' mastery of the nontechnical KSAs covered in the curriculum.

Overall, the data analysis shows that the CAP was influential in developing nontechnical KSAs among students. The program's curriculum design, assessment methods, and andragogical learning elements helped foster these skills development. Therefore, the researchers achieved the purpose of the study, which was to assess the effectiveness of the CAP curricula in developing targeted nontechnical KSAs among bronze-level ambassadors.

However, it is vital to acknowledge the study's limitations and discrepancies in its findings. For example, the study's small sample size limits generalizability. Additionally, the single geographical location may also be a limiting factor. Nonetheless, the findings provide valuable insights into the program's effectiveness in developing nontechnical KSAs and can inform the development of similar programs in the future.

5. Conclusions

The study's findings have several implications for individuals and organizations involved in CS education, training, and awareness.

First, the results provide insight into the effectiveness of the 16-week bronze-level CAP curriculum in developing nontechnical KSAs among bronze-level ambassadors and emphasize the importance of addressing the current CS skills gap.

The data analysis showed that the CAP curriculum design, assessment methods, and elements of andragogical learning could help bridge the CS skills gap and equip individuals with necessary nontechnical KSAs. This finding is significant for individuals seeking to improve their nontechnical KSAs and organizations and institutions seeking to develop the next generation of the CS workforce.

In addition, the study's findings have implications for transformative learning and leading. For example, the CAP curriculum design, which focused on communication, customer service, and stress management, helped foster the development of students' critical thinking and problem-solving skills. These skills are essential for transformative learning and leading, enabling individuals to address complex problems and make informed decisions.

The data generated showed that the demand for CS skills continues to grow. The Bureau of Labour Statistics projects that "employment in computer and information technology occupations is projected to grow 15 percent from 2021 to 2031, much faster than the average for all occupations" [13]. This data highlights the need for individuals to develop and hone nontechnical KSAs to remain competitive in the job market.

Furthermore, the study's findings contribute to the larger literature, knowledge, and practice in CS education and training. Finally, the results provide insights into the effectiveness of nontechnical KSAs in addressing the CS skills gap and offer recommendations for developing similar programs in the future.

This study's findings have practical implications for individuals, communities, organizations, and institutions involved in CS education and training. The results highlight the importance of developing and honing nontechnical KSAs and offer insights into practical methods. The data generated from the proposal also underscore the need for individuals to acquire these skills to meet the growing demand for CS talent. Additionally, the study's findings have implications for transformative learning and leading and contribute to the larger body of literature, knowledge, and practice for CS education and training. For this reason, CAP provides an excellent point of departure for other academic institutions interested in starting their version of the program.

5.1. Implications

The study's findings have several implications for individuals and organizations involved in CS education, training, and awareness. First, the results provide insight into the effectiveness of the 16-week Bronze-level/Tier 1 CAP curriculum in developing nontechnical KSAs among novice students by addressing the current CS skills gap. The team used skills verified by compliance organizations and hiring managers.

Data analysis showed that the CAP curriculum design, assessment methods, and elements of andragogical learning could help bridge the CS skills gap and equip individuals with necessary nontechnical KSAs. This finding is significant for individuals seeking to improve their nontechnical KSAs and organizations and institutions seeking to develop the next generation of the CS workforce. The team also noted a unifying effect that served to nurture students from underrepresented populations – that sense of purpose and belonging supported undergraduate cybersecurity classes where they were the minority.

In addition, the study's findings have implications for transformative learning and leading. For example, the CAP curriculum design, which focused on communication, customer service, and stress management, helped foster the development of students' critical thinking and problem-solving skills. These skills are essential for transformative learning and leading, enabling individuals to address complex problems and make informed decisions. As a result, CAP students achieved student leadership recognition at disproportionately higher rates than their peers.

The data generated from the proposal also showed that the demand for CS skills continues to grow. For example, the Bureau of Labour Statistics projects that "employment in computer and information technology occupations is projected to grow 15 percent from 2021 to 2031, much faster than the average for all occupations" [13]. This employment data highlights the need for individuals to develop and hone nontechnical KSAs to remain competitive in the job market.

Furthermore, the study's findings contribute to the larger body of literature, knowledge, and practice in CS education and training. Finally, the results provide insights into the effectiveness of nontechnical KSAs in addressing the CS skills gap and offer recommendations for developing similar programs in the future.

This research has practical implications for individuals, communities, organizations, and institutions involved in CS education and training. The results highlight the importance of developing and honing nontechnical KSAs and offer insights into practical methods. The data generated from the proposal also underscore the need for individuals to acquire these skills to meet the growing demand for CS talent. Additionally, the study's findings have implications for transformative learning and leading and contribute to the larger body of literature, knowledge, and practice in CS education and training.

5.2. Recommendations

Based on the conclusions drawn from the findings of this study, the following recommendations may improve CS education and training. First, more organizations must develop and implement similar CS education and training programs. Second, organizations and institutions involved in CS education and training should develop and implement programs targeting nontechnical KSAs, such as communication, customer service, stress management, and critical thinking. The 16-week CAP curriculum design, assessment methods, and elements of andragogical learning can serve as a model for developing and implementing such programs aimed at developing these nontechnical KSAs in students with varying degrees of experience. Third, researchers should conduct more studies to adapt such programs based on workforce demands.

Similarly, one cannot overstate the importance of including nontechnical KSAs in CS education and training. CS education and training programs should include nontechnical KSAs to enhance the effectiveness of their training programs. Incentives such as micro-learning and micro-credential opportunities are motivational and ways to assure assessment credibility. Organizations such as the Educational Design Lab (EDL) offer targeted micro-badges, including collaboration, creative problem-solving, critical thinking, oral communication, and resilience, which helped form the CAP curricula assessment tools.

Finally, the program fosters unique collaboration and peer learning, keeping students on track to graduate on time. Organizations and institutions could foster similar cooperation and camaraderie among students. A CAP-like program promotes peer learning, enhancing the effectiveness of its CS education and training programs. Peer learning opportunities, such as those provided by the CAP Podcast and the CAP Cyber Bowl, can promote leadership opportunities and collaborative engagement while developing students' nontechnical KSAs.

5.3. Reflections

This study explored developing and implementing a sixteen-week CAP curriculum targeting nontechnical KSAs. The data showed that this program might effectively improve the acquisition of nontechnical KSAs in participating students. The study highlights the importance of nontechnical KSAs in building a culture of CS and bridging the CS skills gap. The findings suggest that the CAP curriculum can effectively develop students' nontechnical KSAs related to CS and contribute to improved CS awareness and behaviour, ultimately protecting organizations, customers, and assets from cyber threats. This enrichment for any student, especially those from underrepresented populations, provides the cybersecurity workforce with an entry-level worker performing at a higher-than-expected level of competency.

The baseline and progress made by the pilot group showed that nontechnical KSAs play a critical role in cybersecurity education and student confidence. This study underscores the importance of nontechnical KSAs in cybersecurity education and highlights the potential of education and training to bridge the cybersecurity skills gap. In addition, the findings suggest that developing nontechnical KSAs can improve CS awareness and behaviour, ultimately protecting organizations, customers, and assets from cyber threats.

The exploration of curriculum flexibility was a critical aspect of program success. Developers effectively developed content that provided students with a CS context for these nontechnical KSAs. In addition, the sequential and progressive nature of the modules allowed students to apply learning in novel situations. For example, they could improvise while presenting, thus leading to positive customer relations, better use of computers and computing tools, fluid presentation skills, better-written communication skills, working more effectively with peers, adaptability, intellectual curiosity, managing personal stress, and maintaining a professional demeanour. These skills are essential for individuals seeking to pursue a career in cybersecurity and line up well with the next tier as Silver/Tier 2 Cybersecurity Ambassador.

Finally, the CAP curriculum can be adapted and applied in different learning environments. The study highlights the potential of the CAP curriculum to be adapted and used in K-12, community colleges, or technical schools. Additionally, a micro-credential would add incentives and benefit individuals and employers by providing a clear and recognized standard for evaluating job candidates' nontechnical CS skills.

As the literature indicated, the workforce demand for skilled cybersecurity talent has exceeded its supply for numerous consecutive years. Historically, the pedagogical approach was to identify and create curricula for the most in-demand technical knowledge, skills, and abilities (KSAs). However, recent research suggests adding a core set of nontechnical KSAs that employers seek after. This study explores the codification of a nontechnical curriculum for a cybersecurity internship program at the University of Southern Maine (USM). The USM faculty created the Cybersecurity Ambassador Program to serve students and the community. The service to students was to make them more attractive to employers. The benefit to the community was to provide cybersecurity awareness training to vulnerable populations. This discussion about the USM CAP serves as a case study for other programs considering this type of enrichment using an internship model.

CAP started as an informal program but needed repeatable blueprints. The researchers designed these lesson plans to help students progress from novices to competent in crucial nontechnical skills delineated in the National Initiative for Cybersecurity Education (NICE) Workforce framework. The team used a mixed methods approach to baseline Tier 1/novice students' skill levels, place them in a cybersecurity enrichment program, track their progress, and determine program efficacy in helping them achieve beginner status. The information shared can serve as a point of departure for a case study that might guide other programs interested in doing similar work. Overall, this study offers valuable insights into the effectiveness of the CAP curriculum and suggests promising areas for further research and development in cybersecurity education and training. In addition, it provides a valuable contribution to cybersecurity education and training, with potential benefits for individuals, organizations, and communities alike.

Funding

The Maine State Office of Securities, the Maine Technologies Institute, and the Maine Economic Initiative Fund supported this work.

References

[1] V. Marshall, L. Mills, J. Weingard, J. Young, The UK cyber-security strategy: Landscape review, National Audit Office, United Kingdom, 2013. [Online]. Available: https://www.nao.org.uk/reports/the-uk-cyber-security-strategy-landscape-review/. [Accessed: Sep. 19, 2022].

[2] M.E. Armstrong, K.S. Jones, A.S. Namin, D.C. Newton, "Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals," *Association for Computing Machinery (ACM) Transactions on Computing Education*, vol. 20, no. 4, pp. 1–25, 2020, doi: 10.1145/3421254.

[3] K. Cabaj, D. Domingos, Z. Kotulski, A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, vol. *75*, pp. 24–35, 2018, doi: 10.1016/j.cose.2018.01.015.

[4] J. Peeler, "(ISC)^2 Study: Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate," (ISC)^2, 2015. [Online]. Available: https://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html. [Accessed: Nov. 1, 2022].

[5] D.N. Burrell, "An exploration of the cybersecurity workforce shortage," in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, Management Association, Information Resources Ed. Hershey, PA: IGI Global, 2020, pp. 1072–1081, doi: 10.4018/978-1-7998-2466-4.

[6] R.T. Palmer, R.J. Davis, T. Thompson, "Theory meets practice: HBCU initiatives that promote academics success among African Americans in STEM," *Journal of College Student Development*, vol. 51, no. 4, pp. 440–443, 2010, doi: 10.1353/csd.0.0146.

[7] WR Poster, "Cybersecurity needs women," *Nature*, vol. *555*, no. 7698, pp. 577–580, 2018, doi: 10.1038/d41586-018-03327-w.

[8] Federal Trade Commission Report to Congress, *Combating Fraud in African American and Latino Communities*, 2016. [Online]. Available: https://www.ftc.gov/system/files/documents/reports/combating-fraud-african-american-latino-communities-ftcs-comprehensive-strategic-plan-federal-trade/160615fraudreport.pdf. [Accessed: May 22, 2023].

[9] C.M. Cook, J.J. Howard, Y.B. Sirotin, J.L.Tipton, A.R. Vemury, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 1, pp. 32–41, 2019, doi: 10.1109/TBIOM.2019.2897801.

[10] L.L. Sussman, "Exploring Nontechnical Knowledge, Skills, and Abilities (KSA) that May Expand the Expectations of the Cyber Workforce," *Cybersecurity Skills Journal*, pp. 19–39, 2020, [Online]. Available: https://nationalcyberwatchcenter.wildapricot.org/event-4057720. [Accessed: Sept. 30, 2022].

[11] H. Jang, “Identifying 21st century STEM competencies using workplace data,” *Journal of Science Education and Technology,* vol. 25, no. 2, pp. 284 – 301, 2016, doi: 10.1007/s10956-015-9593-1.

[12] S.E. Dreyfus, “The Five-Stage Model of Adult Skill Acquisition,” *Bulletin of Science, Technology & Society,* vol. 24, no. 3, pp. 177 – 181, 2004, doi: 10.1177/0270467604264992.

[13] US Bureau of Labour Statistics. (2022). *Customer Service Representatives: Occupational Outlook Handbook.* [Online]. Available: https://www.bls.gov/ooh/office-and-administrative-support/customer-service-representatives.htm#tab-4 [Accessed: Oct. 27, 2022].