

In this issue:

- 4. A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions**
Cheryl Beauchamp, Regent University
Holly Matusovich, Virginia Tech

- 27. Higher Education Model for Security Literacy using Bloom's Revised Taxonomy**
Gary White, Texas State University

- 37. Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona**
Paul Wagner, University of Arizona
Dalal Alharthi, University of Arizona

- 64. Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation**
Ryan Straight, University of Arizona

The **Cybersecurity Pedagogy and Practice Journal (CPPJ)** is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (<https://cppj.info>). Our sister publication, the proceedings of the ISCAP Conference (<https://proc.iscap.info>) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at <https://iscap.us/papers>. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2024 ISCAP Board of Directors

Jeff Cummings
Univ of NC Wilmington
President

Amy Connolly
James Madison University
Vice President

Eric Breimer
Siena College
Past President

Jennifer Breese
Penn State University
Director

David Gomillion
Texas A&M University
Director

Leigh Mutchler
James Madison University
Director/Secretary

RJ Podeschi
Millikin University
Director/Treasurer

David Woods
Miami University
Director

Jeffry Babb
West Texas A&M University
Director/Curricular Items Chair

Tom Janicki
Univ of NC Wilmington
Director/Meeting Facilitator

Paul Witman
California Lutheran University
Director/2024 Conf Chair

Xihui "Paul" Zhang
University of North Alabama
Director/JISE Editor

Copyright ©2024 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Anthony Serapiglia
Co-Editor
Saint Vincent College

Jeffrey Cummings
Co-Editor
University of North Carolina
Wilmington

Thomas Janicki
Publisher
University of North Carolina
Wilmington

2024 Review Board

Cheryl Beauchamp
Regent University

Ulku Clark
Univ of NC Wilmington

Peter Draus
Robert Morris University

Nick Giacobe
Penn State University

Mike Hills
Penn State University

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Jim Marquardson
Robert Morris University

Stan Mierzwa
Kean University

Etezady Nooredin
University of New Mexico

Ron Pike
Cal Poly Pomona

RJ Podeschi
Milliken University

Samuel Sambasivam
Woodbury University

Kevin Slonka
Saint Francis University

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Ping Wang
Robert Morris University

Tobi West
Coastline College

Johnathan Yerby
Mercer University

A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions

Cheryl Beauchamp
cherbea@regent.edu
Department of Engineering and Computer Science
Regent University
Virginia Beach, VA

Holly Matusovich
matushm@vt.edu
Department of Engineering Education
Virginia Tech
Blacksburg, VA

Abstract

Training a skilled cybersecurity workforce is a complex problem, similar to the challenge of securing cyberspace itself. The National Academy of Engineering identified securing cyberspace as one of the 14 Grand Challenges due to the complexity of cyberspace. This same complexity impacts the ability to effectively recruit and educate cybersecurity students with the necessary knowledge, skills, and abilities to secure these critical and open systems. A growing number of organizations and academic institutions use cybersecurity competitions to increase students' interest and cybersecurity-related knowledge. Although literature exists regarding cybersecurity competitions, current research regarding the participant's perspective is lacking. Using Eccles' Situated Expectancy Value Theory (SEVT), this study explored how students were motivated by participating in cybersecurity Capture the Flag (CTF) competitions. Results found participants who identified as female had a significant variation in expectancy of success compared to those who identified as male. Results also showed that interest and attainment were the SEVT elements of motivation that were most salient for student CTF participants. Responses regarding the CTF utility were more dispersed and relative costs were the lowest construct as students did not believe participation required much preparation or stress. Prior studies claimed that cybersecurity CTF competitions have a high knowledge barrier that discourages wider participation; however, results from this study show that students did not find their lack of cybersecurity knowledge stressful. This study contributes to CTF developers and educators' efforts to build CTFs that successfully engage students in cybersecurity education.

Keywords: cybersecurity education, cybersecurity competition, Situated Expectancy Value Theory, student academic motivation, Cyber CTF.

Recommended Citation: Beauchamp, C., Matusovich, H. (2024). A Mixed-Method Study Exploring Student Motivation for Participating in Cybersecurity CTF Competitions. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.4-26. <https://doi.org/10.62273/QOGS6742>

1. INTRODUCTION

According to Cyberseek, a project supported by the National Initiative for Cybersecurity Education (NICE), over 660,000 cybersecurity positions in the U.S. were unfilled in 2023 (Cyberseek, n.d.). This is an increase from the 300,000 cybersecurity positions that were unfilled in 2018 (National Institute of Standards and Technology, 2018).

Recognizing the national interest to protect our cyber systems, the U.S. Congress passed the Cybersecurity Workforce Assessment Act (Public Law No. 113-246). This Act required the U.S. Department of Homeland Security to develop a plan to increase and train cybersecurity professionals, including designating U.S. higher education institutes as Centers of Academic Excellence in Cyber Defense Education (National Initiative for Cybersecurity Careers and Studies, 2019). A component of this designation requires collegiate participation in industry-supported cybersecurity competitions to engage students, encourage their continued interest in cybersecurity, and provide relevant training and learning opportunities in content and professional skills.

A common and popular type of cybersecurity competition is Capture the Flag (CTF). There are two typical formats of CTF competitions: Jeopardy-style and defense/offense. The Jeopardy-style format is more common and uses a set of questions that reveal clues to guide competitors in their efforts to solve challenges. The challenges are organized such that hints to assist with the follow-on challenges are revealed while solving the initial challenges. Challenges of varying difficulty levels are organized into cybersecurity-related categories such as cryptography, reverse engineering, and forensics. Completing a challenge earns a flag with varying points. A team's CTF score increases as flags are discovered and submitted during the competition, which has a predetermined time limit. Teams earn more points for more complex and time-consuming challenges and use different problem-solving strategies to maximize their success within the competition's time limit. A second format is the defense/offense type of CTF, where, in a common variation, "blue teams" (usually the CTF participants) protect their network from being hacked by the "red team" (usually the CTF organizers or a more experienced team). Teams successfully hack each other by obtaining a flag from their opponent's system, usually a file. This

type of CTF is more challenging to set up and is less common for academic CTFs.

CTF competitions exist online and in-person and are used in cybersecurity education for hands-on experiences that reflect real-world application. They have varying difficulty levels, and competitions are hosted at all levels, including high school. For example, Carnegie Mellon launched their picoCTF competition in 2013 with over 6,000 participants. Their research vision is "Big Learning, Small Challenges - If we cannot make learning cybersecurity easy, then we will make it fun" (About picoCTF, n.d.). The Technology Student Association offered a CTF cybersecurity competition for the first time at their 2019 National TSA conference (Technology Student Association, 2019). Their CTF aligns with their mission of "...accelerating student achievement and supporting teachers by providing engaging opportunities to develop STEM skills" (Technology Student Association Mission, n.d.). Higher education institutions and private organizations also use CTF cybersecurity competitions to engage students and develop their cybersecurity-related skills. National Centers of Academic Excellence in Cybersecurity (NCAE-C) hosted their first cybersecurity CTF competition in 2022 (NCAE Cyber Games, n.d.). According to the CAE Director, the NCAE Cyber Games are for students who have never competed before and is designed to teach students how to the competitions work. It's considered a learning competition to identify the skills they need to compete (email from John Watkins on 11/9/2021).

Although the use of CTF competitions has grown in an effort to engage students and motivate them to learn more about cybersecurity, little is known about how students find these competitions engaging and motivating. Thus, the purpose of this mixed-method study was to explore how undergraduate student motivation is manifested through the lens of Eccles' Situated Expectancy Value Theory (SEVT) for academic motivation (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000; Jones et al., 2009) in the context of students participating in a cybersecurity CTF competition and what variations in motivation may exist due to student demographics. The research questions addressed in this study were the following:

1. Which elements of SEVT are most salient for students in the context of a CTF?
2. What variations in motivation are evident based on student demographics such as

experience level, gender, and program of study?

Using Eccles' SEVT framework (Eccles & Wigfield, 2020), this study explored how undergraduate students who participated in a Virginia Cyber Range (VaCR) hosted CTF were motivated. Responses to an anchored open-ended (AOE) questionnaire were analyzed in terms of expectancy of success and task values such as attainment, interest, utility, and relative costs. Results show that students who participated in a cybersecurity CTF were primarily motivated by their interest-enjoyment of the CTF experience and the professional development opportunities that would help them become cybersecurity specialists. Because participation was voluntary and the format supported learning while competing, many students did not perceive stress to carry with it a noteworthy cost. The only significant variation in motivation when comparing demographics of the CTF participants was the expectancy of success with those who identified as females less confident than those who identified as males.

2. LITERATURE REVIEW

Because CTF-specific research is limited, this review broadly encompasses cybersecurity competition research, of which CTF competitions are a sub-group. Past studies have examined cybersecurity competitions that are similar to CTFs (they include team collaboration to address complex cybersecurity-related challenges in a given time frame). However, these competitions have added complexity in that they simulate actual organization networks and the vulnerabilities that may cause systems to be breached. Teams work together to address the vulnerabilities while also mitigating attacks and breaches. Some studies have focused on the competition event itself, describing objectives, results, and benefits (Conklin, 2005; Cheung et al., 2011), while other studies investigated the types of students who participate in the competitions (Bashir et al., 2015; Bashir et al., 2017). Others have explored competition effectiveness in furthering students' interest in pursuing cybersecurity careers (Tobey et al., 2014, Gavas et al., 2012) and changes in student interest after participating in a competition event (Cheung et al. 2012). More recent studies have investigated aspects of cybersecurity competitions to include experiences of underrepresented populations (Pusey et al., 2016), learning outcomes (Woszczyński & Green, 2017), and professional skills development that includes teamwork and leadership (Buchler, La

Fleur, et al., 2018; Buchler, Rajivan, et al., 2018).

A few studies have specifically explored student motivation. For example, Bashir et al. examined the motivation of students to enter cybersecurity careers after participating in a cybersecurity competition (2017). Bashir's exploratory study surveyed those who participated in the Cybersecurity Awareness Week (CSAW) Conference capture the flag competition at the New York University Polytechnic School of Engineering from 2004 through 2014. The survey captured demographics, competition experience, and career intentions. A significant limitation to the self-efficacy component of their study was reliance on retrospective self-reported data of the participants because participant reports of their perceived self-efficacy on the survey could differ significantly due to the long period from when they participated in the competition (before completing the survey); also (likely) impacting their recollection. A study that captures participants' feedback closer to their competition experience would address this limitation. Also, Cheung's study included students' self-reported interest in computer security after participating in cybersecurity competitions (Cheung et al., 2012). The findings included a positive interest in continued cybersecurity learning; however, the results did not capture how or why they had increased interest in computer security after the cybersecurity competitions.

While these studies provide insight into a competition event, the types of students that compete, and students' prior knowledge, an extensive study of how and in what way students in these cybersecurity competitions are motivated to participate is lacking. As the use of cybersecurity competitions grows, this study, conducted through a motivation-specific lens, contributes to understanding how these CTFs can be enhanced to improve students' motivation to participate which may contribute to furthering their interest in cybersecurity education.

3. THEORETICAL LENS

According to Maehr and Meyer (1997), the investment a person puts forth to reach an outcome is motivation (Ambrose et al., 2010). The persistence and quality of learning behaviors that students put forth in their learning is academic motivation. Students' motivation in the context of learning sustains what they do to achieve their learning and performance goals.

Eccles' SEVT theorizes academic motivation based on the task value and expectancy of

success (Eccles & Wigfield, 2020; Eccles et al., 1983; Wigfield & Eccles, 2000; Jones et al., 2009) associated with the learning experience. Relevant SEVT constructs for this study include expectancy for success, which relates to how confident a student is in their ability to succeed at the task, and subjective task values such as attainment, interest, utility, and relative costs (Hood et al., 2012; Ambrose et al., 2010; Wigfield & Cambria, 2010). Attainment refers to the level of importance placed on performing the task well. Interest, or intrinsic motivation, refers to task enjoyment. Utility refers to the usefulness of the task in the student's future, also referred to as extrinsic motivation. Relative costs refer to how much effort the task will involve, taking away time from other more enjoyable activities.

SEVT was initially developed to explain the motivation of elementary children in mathematics (Eccles et al., 1983); however, it is now widely used throughout education fields (Lawanto et al., 2012; Panchal et al., 2012; Hood et al., 2012; Ertmer et al., 2011; Wigfield & Cambria, 2010; Williams et al., 2016; McGrath et al., 2013; Matusovich et al., 2014; Brown & Matusovich, 2013). Note that SEVT was formerly EVT and prior works within this framework refer to EVT. The expectancy of success and value constructs are generally the same, but the broader situation of the theory has shifted to recognize that success and value beliefs exist within a context, i.e., are situated.

A review of literature revealed no prior studies of student motivation and cybersecurity competitions using SEVT or EVT as the theoretical framework. However, other studies have used Eccles' SEVT framework to explore undergraduate student motivation using a non-traditional teaching and learning approach. Morelock and Peterson used Eccles's five constructs of SEVT to examine undergraduate student motivation during a 10-week augmented reality, non-competitive, puzzle-based game for computer security learning (2018). A 2015 study also utilized SEVT to explore undergraduate student motivation and persistence in biomedical sciences using a communal utility value intervention to biomedical research to broaden participation in science (Brown et al., 2015). Similarly, the current study utilized Eccles' SEVT to understand undergraduate student motivation using an alternative learning approach, CTF competitions, for cybersecurity learning and persistence. Eccles' SEVT's first construct, success, explored student participant confidence in their ability to succeed in the CTF. The second SEVT construct, attainment, was the importance of CTFs in

students becoming cybersecurity specialists. Participation enjoyment was their primary reason for interest, the third SEVT construct, and professional usefulness was the reported central concept for utility, the fourth SEVT construct. The relative costs reflected the fifth construct, perceived costs, incurred by participating in a cybersecurity CTF. Figure 1 depicts the SEVT theoretical framework for this study.

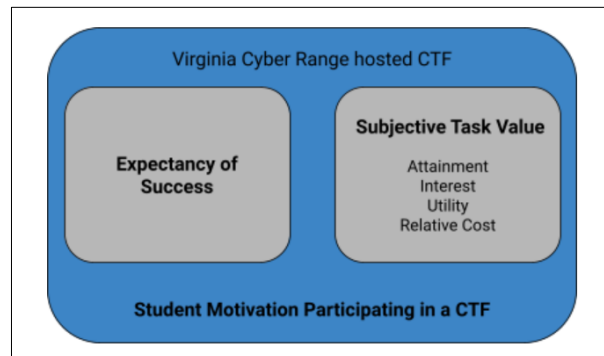


Figure 1: Situated Expectancy Value Theory framework for Student Motivation Participating in a CTF Competition

4. METHODS

Using a concurrent mixed methods approach (Creswell & Creswell, 2018) to explore, compare, and determine evident patterns in the data, this study drew upon the strengths of both quantitative and qualitative methods to understand, from the student perspective, how CTF competitions motivated students. The VaCR was the unit of analysis for this study as the VaCR was the platform for the CTF competitions. The data source was the student responses to an AOE questionnaire that included closed and open-ended items. The open-ended items were anchored with the closed-ended items. They were analyzed concurrently to understand how undergraduate students expect to succeed and value participating in a CTF competition through the constructs of SEVT. Internal Review Board (IRB) approval verified the study aligned with appropriate practices and the researcher attended to ethics.

Data Collection

The primary data source was an anchored open-ended (AOE) questionnaire sent to students who participated in the VaCR hosted Cyber Fusion 2019 or 2020 competition.

Sampling Plan - The sampling used a purposive, non-probability sampling approach (Trochim, 2006) to study students who competed in a VaCR

hosted CTF competition to understand how students were motivated as CTF participants. On April 14, 2021, 224 students who competed in the 2019 or 2020 Cyber Fusion event were invited to complete the questionnaire. Those who participated in both were asked to only reflect on their 2020 experience. Four follow-up emails and an incentive to win via a drawing, one of ten \$50 Amazon gift cards was used to encourage higher response rates. Although 48 students started the questionnaire, 34 to 39 responses were recorded by the end of May 2021 for different questionnaire items.

Anchored Open-Ended Questionnaire - The AOE questions included closed-ended questions that served as foundations (or anchors) for accompanying open-ended questions. Lee & Lutz found that AOE questions provided the ability to sort a large number of responses more quickly than open-ended questions and more accurately than closed-ended questions (2016). The questionnaire, prepared in Qualtrics, included 25 closed-ended questions related to students' expectancy for success and task values rated on a 7-point Likert scale of one (for strongly disagree) to seven (for strongly agree). The instrument, included in Appendix A, also contained nine open-ended questions. These open-ended questions supported participants' ability to describe how the CTF was useful or not useful and how they expected to succeed or not succeed in participating in the CTF competition.

Analysis

The responses to the AOE questions were coded using theoretical a priori and in vivo coding (Miles et al., 2020; Saldana, 2016). The coding used the five constructs of expectancy of success, attainment value, interest value, utility value, and relative costs to identify initial themes and emerging patterns (Wigfield & Eccles, 2000). The open-ended responses were organized by the associated closed-ended items in the survey. They were collated by level of agreement to each closed-ended item within each construct. For the second coding cycle, pattern coding categorized the data by clustering codes with a common overall concept theme. A table organized each closed-ended item of each SEVT construct, which was ordered by level of agreement from the Likert scale. Then the open-ended responses associated with each level of agreement were coded to identify themes that emerged based on responses that agreed at some level, disagreed at some level, or neither agreed or disagreed.

Similar tables were created for all the constructs. The themes for the items within a specific SEVT

construct were then analyzed to identify emerging concepts for that SEVT construct. For example, as seen in Appendix B, Table B.2, themes for expectancy of success were grouped into the emerging concepts of Academic Support, Prior Experience and/or Knowledge, and Team Collaboration.

The closed-ended items were analyzed using an online open-source statistical analysis spreadsheet software, Jamovi (The Jamovi project, 2021). Appendix C provides the results from conducting a reliability analysis for internal consistency of the close-ended items for each construct. Cronbach's alpha was implemented and found the items were internally consistent (Creswell & Poth, 2018). The clustered bar chart for each SEVT construct corroborated the qualitative analysis of the open-ended responses. Concurrently, the concepts that emerged for each SEVT construct through coding provided further insight regarding the findings from the quantitative analysis of the closed-ended items. Concepts were presented per the SEVT construct and were supported with excerpts from the participants and a clustered bar chart from the analysis of the closed-ended questionnaire items. An analysis of variance (ANOVA) test and t-test were used to determine what, if any, variations in motivation were evident based on student demographics (Cohen, Manion, & Morrison, 2018). Jamovi (The Jamovi project, 2021) was used to analyze variations in motivation based on gender identity, prior CTF experience, high school cybersecurity education, and academic program of study. Additionally, assumption checks were also conducted to examine homogeneity of variances.

5. FINDINGS

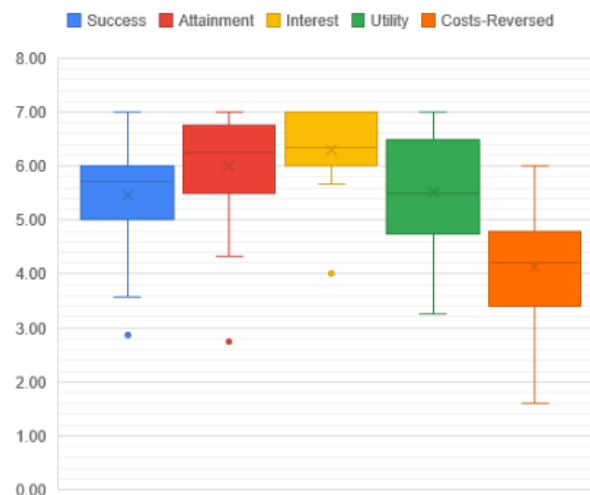


Figure 2: Student Motivation Participating in a Cybersecurity CTF

In addressing the first research question regarding which elements of Eccles' SEVT were most salient for students in the context of a CTF, results showed that interest and attainment were the elements of motivation that were most salient for students in the context of a CTF. Responses regarding the utility of the CTF were more dispersed as students had differing views on the usefulness of participating in a CTF, as seen in Figure 2. Students pursuing cybersecurity-related professions found that participating was useful for professional readiness; however, students who did not see a connection to their future profession did not find CTF participation useful. Relative costs were the lowest construct as students did not believe participation required much preparation or stress.

In addressing the second research question regarding what variations in motivation were evident based on student demographics, results showed that those who identified as female had a significant variation in expectancy of success than those who identified as male. There were no significant variations in motivation due to experience level or program of study.

Motivation per SEVT Construct

Success - Student CTF participants were confident in their ability and skills to compete. As depicted in Figure 3, students were confident in their ability to excel in future CTF activities compared to their ability to excel in their efforts for the current CTF. "That was my first time, I know I could do better if the [CTF Event] even took place this year." When comparing themselves with others, students who were neutral, neither agreeing or disagreeing, stated varying reasons to include no metric for comparison. Some students believed they were better than others but knew others were better than them. Still, others shared that since it was their first time, they could not determine or compare their expectancy of success.

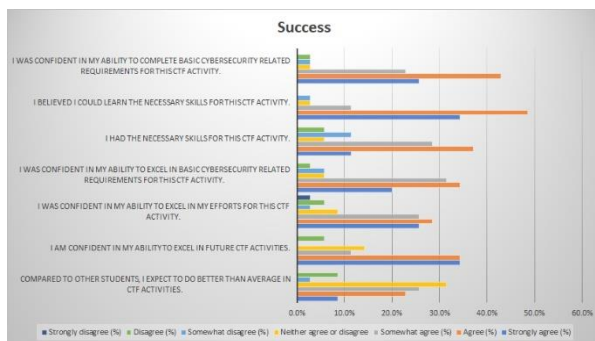


Figure 3: Clustered Bar Chart of Success-Related Closed-Ended Questions

The main themes that emerged through qualitative analysis of all AOE questions combined were prior experience, team collaboration, and academic support. Students who agreed at some level stated that prior experience provided an understanding of what to expect. One student shared,

"I have gotten better and better each CTF that I compete in. This is because each one shows me where I need to work on my skills. For instance, in the NCL, I scored very badly in the Web Application portion this time. I am currently trying to learn more about Web Apps, so next time I will do better."

Additionally, team collaboration provided support and knowledge sharing. Participants were able to focus on subset areas of the competition and relied on other team members to fill in knowledge gaps. One student shared, "My team was structured in such a way where I needed to focus primarily on forensics and reconnaissance challenges. As a result, I knew exactly what I needed to practice before the competition." Some teams had members with varying experience levels in which those with more experience shared their knowledge and understanding with members who had less experience.

Academic support was another source for confidence and expectancy of success. Academic content from the students' university or college provided them relevant knowledge and skills to compete. One participant shared,

"My college degree has given me a solid foundation in cybersecurity concepts, and my competitive cyber club has done a great job compiling problems from a wide variety of sources."

Students who disagreed at some level shared that they did not have any prior experience to draw upon to prepare and compete. A "cannot know what one does not know" theme was shared among those who disagreed with having an expectancy of success: "I had never competed in a cybersecurity competition before, so I did not know what to expect or how to prepare for the competition." Contrary to confident participants, less confident participants shared that they did not have a team strategy in preparing for the CTF competition: "I felt that the [university] cyber team does not prepare for CTFs very well, and almost all of my knowledge was personal

knowledge, so I am always slightly unsure of my ability to perform in a CTF."

Again, similar to team collaboration, a lack of support from academic programs was another reason students disagreed. One student shared, "I did not have the time to learn the skills on my own, and the curriculum at my college was not sufficient to teach me the skills." Another thought they had the foundational knowledge but lacked the hands-on experience that would have provided higher levels of knowledge and relevant skills: "I was able to complete the basic level tasks. I believe that had I been provided more hands-on training by my university I would have been able to complete the more complex tasks."

Attainment - Many student CTF participants agreed they wanted to become cybersecurity specialists (see Figure 4) and being good at solving cybersecurity-related problems was important. Although most agreed that the effort it took for the CTF was worthwhile, they did not agree that they were becoming cybersecurity specialists by participating. For example, one participant noted,

"I have found and know that there is a consensus in the security community, that the tools and tactics used in Jeopardy-style CTF like this one are generally not heavily applicable to specific tasks in most cybersecurity roles. However, they do give familiarity with the general area, and so are not bad as a jumping-off point for many technical roles."

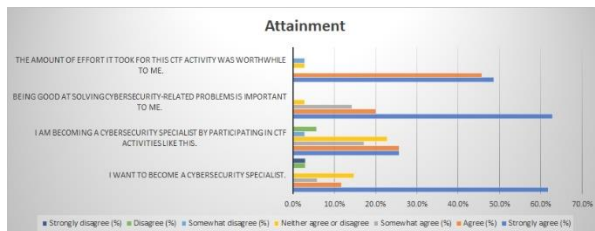


Figure 4 Clustered Bar Chart of Attainment-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the importance of CTFs in becoming a cybersecurity specialist were the alternative approach to learning, the professional readiness development, and the cybersecurity knowledge and skills they obtained. Students who agreed at some level stated that participating in CTFs differed from traditional academic learning (i.e., memorizing content presented in class and then taking a test to demonstrate their understanding). CTFs provided active learning through cybersecurity-related challenges such as

reverse engineering and cryptography. As shared by one of the participants,

"This CTF challenged me to think differently than what is commonly expected in a school environment. School environments expect you to study and then show what you've prepared on a test or exam. At CTF challenges, you come in with perhaps zero experience and learn while you go. It encourages you to come up with different ways of finding answers online instead of just being stumped because you did not prepare for that type of question."

They also stated that CTFs furthered their knowledge and skills by providing exposure to newer areas of cybersecurity, which are essential in the cybersecurity profession as shared by one of the participants, "CTF competitions are good supplemental material for someone seeking a career in cybersecurity because they can act as an indicator of how they are doing in their education and preparation to solve problems by showing which areas they excel at and which they are lagging behind in."

CTF participation also included developing teamwork skills that would be important when working in the profession: "This is also a way of learning different kinds of techniques and skills with teammates. Each of us has a different way of working and thinking ability and we learn from each other which we could use one day at the corporate level."

Students who disagreed at some level shared that CTF participation was not relevant to their future profession. One student shared, "I initially started my journey in IT to become a cybersecurity specialist, but have since decided to pursue the virtualization and cloud areas of IT as those most interest me."

They also disagreed on the importance of CTF participation for supporting their becoming cybersecurity professionals. Some did not believe CTFs alone provided real-world relevant cybersecurity knowledge and skills: "These competitions help us to practice to think critically, under time constraints like in real life jobs. Thus, it is helping us become better in our field by exposing us to the relatable situation. However, I don't think participating in the CTF alone can make anyone a specialist in cybersecurity."

Interest - Most participants found the CTF interesting, exciting, and rewarding, as seen in Figure 5. The content and event, including the career fair, networking, and panel discussion,

contributed to their interest in the event. Competing against others was exciting, and the content was challenging. Many of the students enjoyed the physical system challenges.

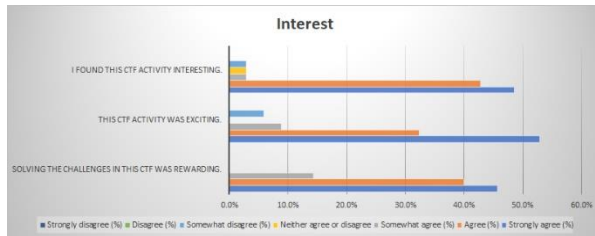


Figure 5 Clustered Bar Chart of Interest-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the interest of participating in a cybersecurity CTF were professional development, team collaboration, and the actual CTF event and content. Students who agreed at some level stated that the CTF demonstrated how cybersecurity knowledge and skills are applied: "It encouraged me to think out of the box and showed the possible challenges while working in the field."

Team collaboration was also why they enjoyed participating as team members with varying knowledge levels and experience shared and helped each other. They found the team effort in the competition was engaging and rewarding: "I love solving problems like the ones offered in this CTF. For 2020, I was also able to help my teammate solve something that he had never seen before. Showing someone is almost as fun as doing it yourself."

The CTF content and format encouraged different approaches and supported different knowledge levels:

"Even though the competition lasted for a few hours, I was totally invested in every second because time went by faster than expected. If I was stuck on a particular problem, I was not forced to figure that one out before moving on, but instead was able to choose what I wanted to solve based on my strengths and interests."

Students also enjoyed the in-person event, which supported networking with cybersecurity professionals and students who had similar interests in cybersecurity from other universities and colleges. One student shared, "This CTF was interesting and exciting as I got to interact with people currently in the cyber field, meet other students, and challenge myself against others to see where I stand."

Students who disagreed did not find the CTF interesting, rewarding, or exciting because, as one student stated, "The CTF challenges were too difficult."

Utility - CTF participants strongly agreed that those who participate in CTFs had more opportunities to succeed, as seen in Figure 6, and participation was useful for post-graduation plans. They also agreed it led to good working opportunities. Those who responded neutrally, neither agreeing or disagreeing, stated that participation was nice to have on their resume; however, they heard that even though CTFs contribute to good problem-solving skills, the tasks themselves would not come up in [actual] security roles. Those who responded neutrally also stated that CTF participation would not provide working opportunities. However, the participation effort demonstrated to future employers the mindset and desire for more growth and learning compared to those who did not participate.

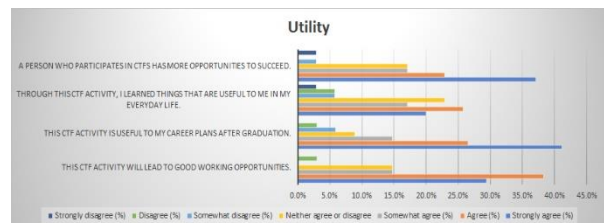


Figure 6 Clustered Bar Chart of Utility-Related Closed-Ended Questions

Professional readiness was the primary theme that emerged across all AOE questions regarding the usefulness of participating in a cybersecurity CTF. Students who agreed at some level shared several utility aspects that contributed to their professional readiness efforts. CTF participation was great resume content: "These are good for putting on a resume to help you find a job." They believed recruiters valued applicants with CTF experience. Furthermore, while some did not believe the actual challenges were real-world relevant, they did think that solving the challenges demonstrated logical and critical thinking skills that were useful in any profession.

Participants also found networking with other CTF attendees and hearing from company representatives on what they were looking for in a future hire useful. One student shared how participating was helpful in their job interviewing process:

"Participating in CTF events gave me a lot of material to talk about when interviewing for jobs."

In addition, the information that I learn from it helps to give context when actually working and talking about defending or attacking systems."

Students who disagreed at some level shared that most CTF challenges do not directly help with future careers. Some believed experience with the technology they would be working with in their future profession would be more useful. One student shared, "I feel like it looks good on a resume, so it may be useful, but my experience with actual technologies will serve me better." Others did not see the connection between the CTF challenges and what would be helpful in the actual profession.

Relative Cost - As seen in Figure 7, many student CTF participants strongly agree that participating in the CTF was difficult and took significant effort. However, this was perceived as a good thing because if it were easy, it would not be challenging, and if it were not challenging, it would not be enjoyable and engaging. Many disagreed that they were stressed or did not have time to do anything else because of the learning-while-doing approach and team support. Having team members as subject matter experts supported a team approach of each member's ability to focus on subject matter strengths. Because they did not know what to expect, participation did not require much time or effort for prior preparation. Instead, it supported the ability to research information while competing, and thus new learning was achieved while competing: learning by doing.

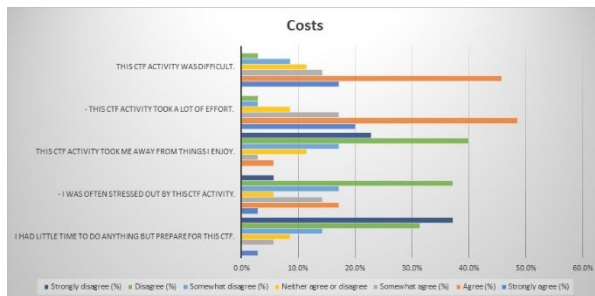


Figure 7 Clustered Bar Chart of Cost-Related Closed-Ended Questions

The main themes that emerged across all AOE questions regarding the costs incurred by participating in a cybersecurity CTF were the difficulty level of the CTF, the effort and time, and the stress of competing. Students who agreed at some level stated that the CTF was difficult, but the primary purpose of the CTF was new learning, which is difficult:

"For me, the purpose of the CTF was to learn. If

it wasn't difficult, it wouldn't have been worth doing, because I wouldn't have learned much. I'm glad it was difficult - it gave me an opportunity to learn, and learning takes effort."

CTF novices found participating stressful because they did not know what they did not know. Their lack of cybersecurity knowledge also contributed to their personal level of difficulty: "The CTF was difficult in terms of skill requirement, I didn't think it was beginner-friendly and required someone who was more adept at hacking."

However, students also believed that difficulty and stress are good things. They did not believe it would be enjoyable or engaging if it were easy. Stress was not always considered a bad thing: "Some of them [challenges] were incredibly difficult which just made solving them even more rewarding." Some participants thought the enjoyment and reward were due to solving complex challenges that required work to figure out: "When you really have to work at an answer, it is satisfying to solve it." CTF stress was considered a good thing that made participation worthwhile: "The CTF was a good kind of stress. If something is easy, it's often not worth doing." Stress during the competition was even considered motivating: "There was occasional stress during the event as time was nearing the end, but the pressure was also motivating."

Students who disagreed at some level shared that participating did not take much prior preparation time or effort:

"I can arguably say there are things I would have enjoyed doing more than the CTF, but the purpose of the CTF wasn't for fun - it was for learning and resume building, no one was expected to come in knowing everything, so it did not take time away from things you enjoy. I personally did not prepare at all for the CTF challenge and still had a great time."

Difficulty and stress are expected during CTFs and contributed positively to the event:

"This CTF activity was difficult, but that is the whole point. CTF competitions are learning experiences created to help students learn how to problem solve, work as a team, focus on time management, etc. So yes, it was difficult and stressful, but that is what pushed people to try their hardest."

Variations in Motivation

When considering the second research question of comparing motivation by gender identity, prior CTF experience, previous high school

cybersecurity education, and academic program of study, the only significant difference with a high effect size was gender identity for expectancy of success as seen in Appendix D. Assumption checks, such as homogeneity tests, were also conducted and did not identify any violation of the assumption of equal variances. Expectancy of success had significant variations, with females having less confidence in their ability to succeed than males, as seen in Figure 8.

Independent Samples T-Test						
		Statistic	df	p		Effect Size
AvgS	Welch's t	2.9293	20.9	0.008	Cohen's d	1.0663
	Mann-Whitney U	56.0		0.006	Rank biserial correlation	0.5758
AvgA	Welch's t	-0.1192	28.7	0.906	Cohen's d	-0.0409
	Mann-Whitney U	127.5		0.884	Rank biserial correlation	0.0341
AvgI	Welch's t	1.2143	13.0	0.246	Cohen's d	0.4795
	Mann-Whitney U	111.0		0.447	Rank biserial correlation	0.1591
AvgU	Welch's t	0.0454	23.7	0.964	Cohen's d	0.0162
	Mann-Whitney U	130.5		0.971	Rank biserial correlation	0.0114
R-AvgC	Welch's t	0.0432	18.8	0.966	Cohen's d	0.0160
	Mann-Whitney U	126.5		0.857	Rank biserial correlation	0.0417

Group Descriptives						
	Group	N	Mean	Median	SD	SE
AvgS	Male	22	5.82	5.86	0.883	0.1882
	Female	12	4.83	5.07	0.974	0.281
AvgA	Male	22	6.03	6.38	0.980	0.2089
	Female	12	6.07	6.13	0.729	0.210
AvgI	Male	22	6.45	6.33	0.443	0.0944
	Female	12	6.06	6.33	1.090	0.315
AvgU	Male	22	5.58	5.50	1.078	0.2299
	Female	12	5.56	5.75	1.029	0.297
R-AvgC	Male	22	4.10	4.10	0.919	0.1960
	Female	12	4.08	4.40	1.152	0.333

Figure 8: Variation in Motivation by Gender

Limitations

The main limitation of this study was that the data was from a specific CTF, which limited student participation to those at universities and colleges designated by the National Security Agency and Department of Homeland Security as Centers of Academic Excellence in Cybersecurity. These students were attending institutions recognized for their exceptional cybersecurity academic programs. Thus, the students may have considerable prior knowledge, experience, and preparation for these CTFs compared to other students who participated in other CTFs. Additionally, CTF events themselves vary with different supporting events and format, therefore, the results will reflect findings from this specific CTF event and future studies of other CTFs would address this limitation by comparing the student motivations in other CTF events for similarities and differences to this study.

Another limitation of this study was the low response rate because most students registered for the CTF with their school email account. Those who graduated in 2019 or 2020 may not maintain

their school account and thus would not have received the invitation to participate in this study. Initially, the study plan included participants from the 2021 event; however, due to COVID, the 2021 CTF event was canceled, requiring the sample to draw from 2019 and 2020 participants.

6. DISCUSSION

Findings from this study align with prior studies regarding interest and team collaboration. Students found cybersecurity CTF competitions motivating due to their interest-enjoyment and professional readiness development from participating. Strategic team collaboration also contributed to students' interest and confidence in participating. However, contrary to prior studies regarding negative student experience due to CTF difficulty, the findings from this study reveal that although most students found CTFs to be difficult and stressful, this difficulty was not a negative factor of CTFs, but rather a positive one. They shared that solving complex challenges was more rewarding because easy challenges would not be worth the effort or satisfying to solve. Thus, pressure and stress were considered motivating factors of CTF participation.

Novices found their lack of prior knowledge and experience to be stressful as they did not know what they did not know; however, CTFs supported learning while doing. Thus, prior preparation was not a relative cost as they could gather information and learn while competing.

A study by Cheung and colleagues (2012) focused on changes in interest after participating in a CTF with a finding of student self-reported interest in computer security after participating in cybersecurity competitions. The findings from this study align with Cheung and colleagues' findings as interest was the most salient of the five SEVT constructs. Cheung et al. did not explore why students had a greater interest in cybersecurity after participating in a CTF competition. The findings from this study were that students found participating interesting, rewarding, and exciting due to aspects of the event, the challenges themselves, and the professional development opportunity to network and collaborate with a team.

Buchler and colleagues' study (2018) of team collaboration in a cybersecurity defense competition indicated effective collaboration within teams was an important factor in determining the team's competition success. Although this study did not examine students' motivation in relation to their team's overall

competition success, team collaboration was one of the primary concepts regarding CTF participants' expectancy of success and confidence. This finding aligns similarly to other prior studies that found students value the opportunity to network with other students and potential future employers (Buchler et al., 2018; Gavvas et al., 2012).

Because of the voluntary participation of the students, the relative costs were low. Prior studies claimed that cybersecurity CTF competitions have an extremely high knowledge barrier that discouraged wider participation of students who have limited cybersecurity-related proficiency (Mirkovic et al., 2015; Tobey et al., 2014). Findings from this study show that students did find their lack of cybersecurity knowledge stressful. They agreed that CTFs were difficult and took time and effort. They also reported that not knowing what to expect in the CTF competition prevented them from pre-CTF preparation. However, they also shared that they appreciated the alternative approach to learning while doing and collaborating with more experienced team members who assisted their competition efforts to investigate solutions while competing. The stress and difficulty were reported as positive aspects that made the competition worthwhile. CTFs that were too easy were not considered rewarding.

Students also reported that participating provided new learning, identification of knowledge gaps, and more confidence for the next CTF. Students' expectancy of success in future CTFs after participating in one or more CTFs seemed contrary to prior findings that CTFs discouraged students' participation among those with limited cybersecurity-related knowledge (Cheung et al., 2012).

7. CONCLUSION

Although students reported professional readiness as the central concept regarding the usefulness of participating, the agreement level was widely dispersed. Students in technical disciplines, such as information technology, may not connect the usefulness of cybersecurity education to their discipline. Thus, they may not perceive their participation in cybersecurity-related competitions as valuable for their professional development. However, an understanding of cybersecurity is needed at some level in most technology-related disciplines. More and more technological devices connect to the Internet, and the continued growth in connectedness increases the need for

cybersecurity against possible threats. Cybersecurity is not limited to only those who study cybersecurity or computer science.

Further research is needed to understand why students may not connect the usefulness of CTFs to other programs of study. Additionally, research is also necessary to understand the preparation and resource needs of students who lack prior CTF experience. Although the students reported that the CTF content and format supported different knowledge levels and approaches, those who competed for the first time did not know what to expect and thus did not prepare before the competition. Students also stated they enjoyed the in-person event as it supported networking with professionals and other students and working with physical devices. As more remote CTFs become available, such as TryHackMe and HackTheBox, additional research is needed to compare how students are motivated to participate in virtual CTF competitions versus in-person events.

As more and more universities engage in online and in-person cybersecurity education competitions, research is needed to understand how these competitions motivate student participants. This understanding provides student experience information to the cybersecurity CTF developers and those in the cybersecurity education community who use CTFs for cybersecurity learning and engagement. The AOE questionnaire from this study may serve as a post-CTF assessment tool to provide feedback to CTF developers and facilitators. The AOE questionnaire organizes student responses in specific expectancy constructs of success and value beliefs that support CTF improvement efforts.

Future studies will include examining motivation differences among diverse student populations, varying experience levels, different CTF event formats, and student motivation using other cyber range applications. Studies of other cyber range academic applications exist (Cruz & Simões, 2021; Chouliaras et al., 2021; Larrucea & Santamaria, 2020). These studies examine applications used in higher education while studies of cyber range applications in K12 and student motivation using cyber range resources for cybersecurity education are lacking. Further studies are needed to address the existing gap in understanding how cyber ranges in cybersecurity education motivate students not only as CTF competition participants, but as students who may or may not persist in cybersecurity education.

8. ACKNOWLEDGEMENTS

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

9. REFERENCES

- About picoCTF*. (n.d.) picoCTF. Retrieved January 11, 2022, from <https://picocftf.org/about>.
- Ambrose, S. A., Bridges, M. W., DiPietro, M., Lovett, M. C., & Norman, M. K. (2010). *How learning works: Seven research-based principles for smart teaching*. San Francisco, CA: Jossey-Bass.
- Bashir, M., Lambert, A., Guo, B., Memom, N., & Halevi, T. (2015). Cybersecurity competitions: The human angle. *IEEE Computer and Reliability Societies*, 74-79. <https://doi.org/10.1109/MSP.2015.100>
- Bashir, M., Wee, C. Memom, N., and Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, 65, 153-165. <https://doi.org/10.1016/j.cose.2016.10.007>
- Brown, P. R. & Matusovich, H. M. (2013). Unlocking student motivation: Development of an engineering motivation survey. *American Association Annual Conference & Exposition*, Atlanta, June 23-26, 2013. <https://doi.org/10.18260/1-2-22669>
- Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P. Marusich, L., & Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in Psychology*, 9, Article 2133. <https://doi.org/10.3389/fpsyg.2018.02133>
- Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observation assessment of teaming and leadership in a cyber security defense competition. *Computers & Security*, 73, 114-136. <https://doi.org/10.1016/j.cose.2017.10.013>
- Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). *Challenge Based Learning in Cybersecurity Education*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- Cheung, R, Cohen J, Lo H, Elia F, Veronica CM. (2012). Effectiveness of cybersecurity competitions. *Proceedings of the International Conference on Security and Management*. Las Vegas (NV). <https://worldcomp-proceedings.com/proc/p2012/SAM6108.pdf>
- Chouliaras N, Kittes G, Kantzavelou I, Maglaras L, Pantziou G, Ferrag MA. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11(4), 1809. <https://doi.org/10.3390/app11041809>
- Cohen, L., Manion, L. & Morrison, K. (2018). *Research methods in education* (8th ed.). New York, NY: Routledge.
- Conklin, A. (2005) The use of a collegiate cyber defense competition in information security education. In Proceedings of the 2nd annual conference on Information security curriculum development (InfoSecCD '05). Association for Computing Machinery, New York, NY, USA, 16-18. <https://doi.org/10.1145/1107622.1107627>
- Creswell, J. W. & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*, (5th ed.). Thousand Oaks, CA: Sage.
- Creswell, J. W. & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Thousand Oaks, CA: Sage.
- Cruz, T. & Simões, P. (2021). Down the rabbit hole: Fostering active learning through guided exploration of a SCADA cyber range. *Applied Sciences*, 11(20), 9509. <https://doi.org/10.3390/app11209509>
- Cyberseek. (n.d.). *Hack the gap*. <https://www.cyberseek.org>
- Eccles, J. S., Adler, T.F., Futterman, R., Goff, S. B., Kaczala, C. M., Meece, J. L., & Midgley, C. (1983). *Expectancies, values, and academic behaviors*. In J. T. Spence (Ed.), *Achievement and achievement motivation: Psychological and sociological approaches*, 75 - 146. San Francisco, CA: W. H. Freeman.
- Eccles, J. S. and Wigfield, A. (2020). From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary Educational Psychology*, 61, 101859. <https://doi.org/10.1016/j.cedpsych.2020.101859>

- Ertmer, P. A., Newby, T. J., Liu, W., Tomory, A., Yu, J. H., & Lee, Y. M. (2011). Students' confidence and perceived value for participating in cross-cultural wiki-based collaborations. *Education Technology Research and Development, 59*(2), 213-228. <https://www.jstor.org/stable/41414935>
- Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy, 10*(4), 75-79. <https://doi.org/10.1109/MSP.2012.112>
- Hood, M., Creed, P. A., & Neumann, D. L. (2012). Using the expectancy value model of motivation to understand the relationship between student attitudes and achievement in statistics. *Statistics Education Research Journal, 11*(2), 72-85. <https://doi.org/10.52041/serj.v11i2.330>
- Jones, B.D., Paretto, M.C., Hein, S.F. & Knot, T.W. (2010). An analysis of motivation constructs with first-year engineering students: Relationships among expectancies, values, achievement, and career plans. *Journal of Engineering Education, 99*(4), 319-336. <http://dx.doi.org/10.1002/j.2168-9830.2010.tb01066.x>
- Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods*. (3rd ed.) Long Grove: Waveland Press.
- Larrucea, X., Santamaría, I. (2020). Designing a cyber range exercise for educational purposes. In M. Yilmaz, J. Niemann, P. Clarke, & R. Messnarz (Eds.), *Communications in Computer and Information Science, 1251*. Springer. https://doi.org/10.1007/978-3-030-56441-4_22
- Lawanto, O., Santoso, H. B., & Liu, Y. (2012). Understanding of the relationship between interest and expectancy for success in engineering design activity in grades 9-12. *Educational Technology & Society, 15*(1), 152-161. https://www.researchgate.net/publication/285919614_Understanding_of_the_Relationship_between_Interest_and_Expectancy_for_Success_in_Engineering_Design_Activity_in_Grades_9-12
- Lee, W. C., & Lutz, B. D. (2016). An anchored open-ended survey approach in multiple case study analysis. Paper presented at the ASEE Annual Conference and Exposition, New Orleans, LA. <https://doi.org/10.18260/p.26566>
- Maehr, M.L. & Meyer, H.A. (1997). Understanding motivation and schooling: Where we've been, where we are, and where we need to go. *Educational Psychology Review, 9*, 371-409. <https://doi-org.ezproxy.lib.vt.edu/10.1023/A:1024750807365>
- Matusovich, H. M., Paretto, M. C., McNair, L. D., & Hixson, C. (2014). Faculty motivation: A gateway to transforming engineering education. *Journal of Engineering Education, 103*(2), 302-330. <https://doi.org/10.1002/jee.20044>
- McGrath, C. A, Gipson, K, Pierrako, O., Nagel, R., Papas, J., & Peterson, M. (2013). An evaluation of freshman engineering persistence using expectancy-value theory. 2013 *IEEE Frontiers in Education Conference (FIE)*. Oklahoma City, OK, 23-26 October 2013, 1644-1650. <http://dx.doi.org/10.1109/FIE.2013.6685117>
- Miles, M. B., Huberman, A. M., & Saldana, J. (2020). *Qualitative data analysis* (4th ed.). SAGE Publications.
- Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. 2015 *USENIX Summit on Gaming, Games, and Gamification in Security Education*. August 11, 2015, Washington, D.C., USA. <https://www.usenix.org/conference/3gse15/summit-program/presentation/mirkovic>
- Morelock, J. & Peterson, Z. (2018) Authenticity, ethicality, and motivation: A formal evaluation of a 10-week computer security alternate reality game for CS undergraduates. In 2018 *USENIX Workshop on Advances in Security Education*. Baltimore, MD. USENIX Association. https://www.researchgate.net/publication/331024947_Authenticity_Ethicality_and_Motivation_A_Formal_Evaluation_of_a_10-week_Computer_Security_Alternate_Reality_Game_for_CS_Undergraduates
- NCAE Cyber Games. (n.d.). NCAE Cyber Games. Retrieved on January 11, 2022, from <https://www.ncaecybergames.org/>
- National Initiative for Cybersecurity Education. (n.d.). *Cybersecurity supply/demand heat map*. Cyberseek.

- <https://www.cyberseek.org/heatmap.html>
- National Institute of Standards and Technology, (2018, August 27). *NIST general information*. NIST. <https://www.nist.gov/>
- Panchal, J. H., Adesope, O., & Malak, R. (2012). Designing undergraduate design experiences: A framework based on the Expectancy-Value Theory. *International Journal of Engineering Education*, 28(4), 871-879. <https://api.semanticscholar.org/CorpusID:198188815>
- Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented population. *IEEE Security & Privacy*, 14(6), 90-95. <http://dx.doi.org/10.1109/MSP.2016.119>
- Saldana, J. (2016). *The coding manual for qualitative researchers*. SAGE Publications.
- Technology student association launches cybersecurity and ITF+ certification competitions*. (2019). Technology Student Association. https://tsaweb.org/docs/default-source/computer-science/technology-student-association-announces-cybersecurity-and-itf-competitions.pdf?sfvrsn=a2700d6b_0
- The Jamovi project. (2021). *Jamovi* (Version 1.6) [Computer Software]. <https://www.jamovi.org>
- Tobey, D.H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. *ACM Inroads*, 5(1), 53-6. <https://doi.org/10.1145/2568195.2568213>
- Trochim, William M. (2006). *The Research Methods Knowledge Base*, 2nd Ed. at URL: Watkins, J. (2021, November 9). Community-wide email.
- Wigfield, A., & Cambria, J. (2010). Expectancy-value theory: Retrospective and prospective. In Urdan, T. C., & Karabenick, S. A. (Eds), *The decade ahead: Theoretical perspectives on motivation and achievement*, 16, 35-70. Bingley, UK: Emerald Group Publishing Limited.
- Wigfield, A., & Eccles, J. S. (2000). Expectancy-value theory of achievement motivation. *Contemporary Educational Psychology*, 25(1), 68-81. <https://doi.org/10.1006/ceps.1999.1015>
- Williams, S. A., Lutz, B., Hampton, C., Matusovich, H. M., & Lee, W. C. (2106). Exploring student motivation towards diversity education in engineering. *2016 IEEE Frontiers in Education Conference (FIE)*. Erie, PA, 12-15 October 2016, 1-5. <http://dx.doi.org/10.1109/FIE.2016.7757565>
- Woszczyński, A. B. & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education*, 28(1), 21-42. <http://jise.org/Volume28/n1/JISEv28n1p21.html>

Editor's Note:

This paper was selected for inclusion in the journal as the ISCAP Cybersecurity 2023 Best Paper. The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2023.

APPENDIX A

Anchored Open-Ended Questionnaire for Students

State your level of agreement on a scale of 1 (strongly disagree), 2 (disagree), 3 (somewhat disagree), 4 (Neither agree or disagree), 5 (somewhat agree), 6 (agree), and 7 (strongly agree), to the following statements, where applicable.

Expectancy beliefs

Success

1. I was confident in my ability to complete basic cybersecurity related requirements for this CTF activity.
2. I believed I could learn the necessary skills to complete this CTF activity.
3. I had the necessary skills to complete this CTF activity.
4. Please explain why you were or were not confident in your ability to learn and have the necessary skills to complete this CTF:
5. I was confident in my ability to excel in basic cybersecurity related requirements for this CTF activity.
6. I was confident in my ability to excel in my efforts towards this CTF activity.
7. I am confident in my ability to excel in future CTF activities.
8. Please explain why you were/were not confident in your ability to excel in the basic cybersecurity related requirements for this CTF and in your general efforts towards this and future CTFs:
9. Compared to other students, I expect to do better than average in CTF activities.
10. Please explain why:

Value beliefs

Attainment Value

11. The amount of effort it took to participate in this CTF activity was worthwhile to me.
12. Being good at solving cybersecurity-related problems is important to me.
13. Please explain why the effort to participate in this CTF and being good at solving cybersecurity related problems is or is not worthwhile and important to you.
14. I am becoming a cybersecurity specialist by working on CTF activities like this.
15. I want to become a cybersecurity specialist.
16. Please explain why you are or are not becoming a cybersecurity specialist by working on CTF activities like this and include why you want or do not want to become a cybersecurity specialist.

Interest Value

17. I found this CTF activity interesting.
18. This CTF activity was exciting.
19. Please explain why you or why you didn't find this CTF activity interesting and/or exciting.
20. Solving the challenges in this CTF was rewarding.
21. Please explain why solving the CTF challenges was or was not rewarding and why the activity was or was not intellectually rewarding.

Utility Value

22. This CTF activity is useful to my career plans after graduation.
23. This CTF activity will lead to good working opportunities.

24. Please explain why this CTF activity is or is not useful for your post-graduation career plans or other good working opportunities.
25. A person who participates in CTFs has more opportunities to succeed.
26. Through this CTF activity I learned things that are useful in my everyday life.
27. Please explain why this CTF activity helped or didn't help you learn things that are useful in your everyday life and why CTF participation will or will not provide more opportunities to succeed.

Relative Costs

28. This CTF activity was difficult.
29. This CTF activity took a lot of effort.
30. This CTF activity took me away from things I enjoy.
31. I was often stressed out by this CTF activity.
32. I had little time to do anything but prepare for this CTF.
33. If you found this CTF activity difficult, stressful, took a lot of effort, or time away from things you enjoy, please explain why.

Other information

34. How many CTFs have you participated in?
(per each CTF) How well did your team do (top half or bottom half)?
35. Why did you choose to participate in this CTF?
36. Please note here anything else you would like to share, such as what you would recommend to improve CTFs or whether or not you would recommend CTFs and why.

37. Did you have any prior cybersecurity education while in high school? (This may have been included in a programming, computer science, or networks course). Yes No

If yes, please list the high school cybersecurity education experiences and duration of each experience:

38. Do you have prior high school CTF experience? Yes No

If yes, please list the high school CTF experience(s) and include the years of the experience.

39. Please select your undergraduate program(s) of study: Cybersecurity, Computer Science, Computer Engineering, Interdisciplinary, Information Systems, Other:

40. Years of Undergraduate Study:

41. How do you describe your gender identity? Male, Female, Prefer to self-describe; below:

42. With which racial group(s) do you identify? (Mark all that apply) American Indian or Alaska Native; Hispanic, Latino, or Spanish origin; White; Black or African American; Asian; Middle Eastern or North African; Native Hawaiian or Other Pacific Islander; Another race or ethnicity not listed above

APPENDIX B
Example of Coding Expectancy of Success

Open-ended responses to: Please explain why you were or were not confident in your ability to learn and have the necessary skills to complete this CTF:	Initial coding and thematic coding
Agree	
<p>I had performed well in other collegiate ctf events, and knew that this event's challenges were designed to be learning-focused and that the event itself would not be particularly hard. In addition, our school has a level of built-up ctf-specific knowledge, and so we were able to share tools and tactics among each other beforehand.</p>	<p>P - prior experience - prior CTF Experience, P - Knowledge of what to expect - knew this event was designed to be learning focused and wouldn't be particularly difficult, P-team/club collaboration to prepare - existing team to capture tactics and tools for prior preparation, P - Prior preparation - work with a school team sharing tools and tactics beforehand, P- team sharing of knowledge, tools, and tactics - sharing of tools and tactics between team members beforehand.</p>
<p>My team was structured in such a way where I need to focus primarily on forensics and reconnaissance challenges. As a result, I knew exactly what I needed to practice before the competition.</p>	<p>P-team sharing of knowledge, tools, and tactics - team approach of assigned SME so everyone knew what to prepare for and did not need to prepare for everything</p>
<p>I had participated in many CTF activities before. The skills I did not have were in 2019, there was a Software Defined Radio section that I did not know, but attempted to learn during the event.</p>	<p>P- prior experience: participated in many CTFs, P- learn while doing: Skills that didn't have (Software Defined Radio section), attempted to learn about during the event.</p>
Somewhat Agree	
<p>I had never competed in a Cybersecurity competition before so I did not know what to expect or how to prepare for the competition.</p>	<p>C-lack of CTF Experience, C-Novice, C-lack of prior prep - first time with no understanding of what to expect or how to prepare lack of prior prep</p>
<p>I believe that I had the basic skills necessary to compete because of the classes provided from my educational institution as well as the extra-curricular activities that I participated in. I do believe that I could have done more to prepare and learn but I was unable to due to circumstances not related to my academic career.</p>	<p>P - prior relevant courses/classes, P-prior preparation: extracurricular activities helped with basic skills, felt they could have done better with more preparation but was unable to do so due to circumstances not related to their academic career.</p>
<p>There were a few surprise categories that we knew nothing about and had no chance to prepare</p>	<p>C - can't prepare for CTF surprise challenges: unknown categories prevented prior prep</p>
<p>It was my first actual CTF competition, and I had only just started participating in cyber activities a few months before.</p>	<p>C-novice, C-lack of CTF experience: first CTF competition and had only just started participating in cyber activities a few months prior.</p>
Strongly Agree	

Being my 2nd CyberFusion competition, I felt that I had a good grasp on the type of questions that I would see and I was correct.	P- prior CTF experience: Being my 2nd CyberFusion competition, I felt that I had a good grasp on the type of questions that I would see and I was correct.
I've done countless ctfs before and had won this ctf before	P -prior experience: countless CTFs before and have won this prior CTF
Neither Agree or Disagree	
I was not that confident in my ability to have all the necessary skills for this CTF because I felt as though I did not have the same skill level as the other participants .I feel like their skill sets were more advanced.	Not confident in having all the necessary skills due to others having more advanced skills: C - lack of more advance skills for the complex challenges
Disagree	
Before the VMI CTF, I had participated in various other CTFs such as ones at UVA, ODU, and the University of Richmond. Since I had prior experiences with competing CTFs, I was already comfortable with the idea of learning new things and working on new challenges.	P-Prior experience - prior CTF experience provided confidence with the idea of learning new things and working on new challenges confident in ability to learn
I'm a newbie :)	C-novice: I'm a newbie
Somewhat Disagree	
As an older student, I did not have the time to learn the skills on my own, and the curriculum at my college was not sufficient to teach me the skills.	C-lack of prior prep, C - lack of time - as an older student didn't have time to learn skills on their own. C - Coursework does not provide relevant preparation - curriculum at their college was not sufficient to teach them the skills
Nothing negative; just with time constraints and new challenges it required a lot of skills that I did not have. This is the nature of competition, however! I would not change this!	C - lack of more advanced skills: nothing negative as it is the nature of a CTF and wouldn't change it but the new challenges and time constraint required a skill level that they did not have.
That was my first time. I know I could do better if the Cyber Fusion event took place this year.	C-novice, P-confident in ability to compete in CTF: That was my first time, I know I could do better if the Cyber Fusion event took place this year.

Appendix Table B1: Initial Coding of Expectancy of Success: I had the necessary skills for this CTF activity

Academic Support	Prior Knowledge and/or Experience	Team Collaboration
C - Academic preparation is lacking	C - Can't know what you don't know	C - Lack of team collaboration
P - Prior academic preparation	P - Knowledge of what to expect	P - Team collaboration

C - Coursework does not provide relevant preparation	P - Prior experiences	P - Team effort
C - Not enough hands-on in course work to complete more complex CTF tasks	C - newbie/novice	P - Team sharing of knowledge, tools, and tactics
P - prior relevant courses/classes	C - Can't prepare for CTF surprise challenges	P - Team/club collaboration to prepare
	C - Didn't know what to expect	
	C - Lack of CTF Experience	
	C - No team collaboration of preparation	
	C - Not confident in CTFs due to not knowing what is not known	

Appendix Table B2: Second Level Coding of Expectancy of Success Themes

APPENDIX C
Analysis of Reliability

Reliability Analysis	
Motivation Construct	Scale Reliability Statistics Cronbach's α
Success	0.893
Attainment	0.685*
Interest	0.754
Utility	0.731
Costs	0.754

*According to Taber (2018), the traditional threshold of 0.7 indicated acceptable reliability and lower Cronbach's alpha coefficients were also considered acceptable when the instrument had a smaller number of items. Such that the 0.685 for Interest is acceptable given three items associated with this construct.

APPENDIX D
Variations in Student Motivation Participating in a Cybersecurity CTF

Independent Samples T-Test						
		Statistic	df	p		Effect Size
AvgS	Welch's t	2.9293	20.9	0.008	Cohen's d	1.0663
	Mann-Whitney U	56.0		0.006	Rank biserial correlation	0.5758
AvgA	Welch's t	-0.1192	28.7	0.906	Cohen's d	-0.0409
	Mann-Whitney U	127.5		0.884	Rank biserial correlation	0.0341
AvgI	Welch's t	1.2143	13.0	0.246	Cohen's d	0.4795
	Mann-Whitney U	111.0		0.447	Rank biserial correlation	0.1591
AvgU	Welch's t	0.0454	23.7	0.964	Cohen's d	0.0162
	Mann-Whitney U	130.5		0.971	Rank biserial correlation	0.0114
R-AvgC	Welch's t	0.0432	18.8	0.966	Cohen's d	0.0160
	Mann-Whitney U	126.5		0.857	Rank biserial correlation	0.0417

Group Descriptives						
	Group	N	Mean	Median	SD	SE
AvgS	Male	22	5.82	5.86	0.883	0.1882
	Female	12	4.83	5.07	0.974	0.281
AvgA	Male	22	6.03	6.38	0.980	0.2089
	Female	12	6.07	6.13	0.729	0.210
AvgI	Male	22	6.45	6.33	0.443	0.0944
	Female	12	6.06	6.33	1.090	0.315
AvgU	Male	22	5.58	5.50	1.078	0.2299
	Female	12	5.56	5.75	1.029	0.297
R-AvgC	Male	22	4.10	4.10	0.919	0.1960
	Female	12	4.08	4.40	1.152	0.333

Appendix Figure D1: T-Test Analysis Results Comparing Students by Gender Identity

Independent Samples T-Test						
		Statistic	df	p		Effect Size
AvgS	Welch's t	-1.1693	32.9	0.251	Cohen's d	-0.3895
	Mann-Whitney U	117		0.319	Rank biserial correlation	0.2041
AvgA	Welch's t	-0.5685	31.1	0.574	Cohen's d	-0.1928
	Mann-Whitney U	135		0.696	Rank biserial correlation	0.0816
AvgI	Welch's t	-1.2704	31.4	0.213	Cohen's d	-0.4119
	Mann-Whitney U	125		0.457	Rank biserial correlation	0.1497
AvgU	Welch's t	-1.3447	32.0	0.188	Cohen's d	-0.4526
	Mann-Whitney U	114		0.272	Rank biserial correlation	0.2245
R-AvgC	Welch's t	0.0385	23.2	0.970	Cohen's d	0.0136
	Mann-Whitney U	141		0.853	Rank biserial correlation	0.0408

Appendix Figure D2: T-Test Analysis Results Comparing Students with Prior High School Cybersecurity Education Experience to Those Without

Independent Samples T-Test						
		Statistic	df	p		Effect Size
AvgS	Welch's t	1.5706	9.34	0.150	Cohen's d	0.6864
	Mann-Whitney U	59.0		0.070	Rank biserial correlation	0.43269
AvgA	Welch's t	-0.6769	25.65	0.505	Cohen's d	-0.2234
	Mann-Whitney U	101.5		0.935	Rank biserial correlation	0.02404
AvgI	Welch's t	0.3928	8.83	0.704	Cohen's d	0.1756
	Mann-Whitney U	103.0		0.983	Rank biserial correlation	0.00962
AvgU	Welch's t	-0.0807	13.07	0.937	Cohen's d	-0.0315
	Mann-Whitney U	103.0		0.984	Rank biserial correlation	0.00962
R-AvgC	Welch's t	0.8215	11.12	0.429	Cohen's d	0.3372
	Mann-Whitney U	91.5		0.625	Rank biserial correlation	0.12019

Appendix Figure D3: T-Test Analysis Results Comparing Students with Prior Cybersecurity CTF Experience to Those Without

ANOVA - AvgS						
	Sum of Squares	df	Mean Square	F	p	η^2
Program	4.41	6	0.735	0.686	0.663	0.128
Residuals	30.03	28	1.073			

ANOVA - AvgA						
	Sum of Squares	df	Mean Square	F	p	η^2
Program	3.34	6	0.556	0.640	0.697	0.121
Residuals	24.31	28	0.868			

ANOVA - AvgI						
	Sum of Squares	df	Mean Square	F	p	η^2
Program	1.72	6	0.287	0.478	0.819	0.093
Residuals	16.80	28	0.600			

ANOVA - AvgU						
	Sum of Squares	df	Mean Square	F	p	η^2
Program	7.02	6	1.17	1.01	0.436	0.179
Residuals	32.28	28	1.15			

ANOVA - R-AvgC						
	Sum of Squares	df	Mean Square	F	p	η^2
Program	5.42	6	0.903	0.868	0.530	0.157
Residuals	29.12	28	1.040			

Appendix Figure D4: ANOVA Analysis Results Comparing Student Degree Programs (Computer Science, Cybersecurity, Cybersecurity and Computer Science, Computer Engineering, Information Systems, and Other)

Higher Education Model for Security Literacy using Bloom's Revised Taxonomy

Garry L. White
gw06@txstate.edu
Department of Computer Information Systems
and Quantitative Methods
Texas State University – San Marcos
San Marcos, TX 78666

ABSTRACT

This paper presents and explains a model for the design and content of cyber security literacy curricula for postsecondary education and how Bloom's Revised Taxonomy supports a model of teaching different levels of information security programs at different levels of higher education. Specifically, this paper shows three different security literacy levels (awareness, training, education) for the six different cognitive levels as defined by Bloom's Taxonomy and applies them to different levels of postsecondary education. A summary table is presented to show how and why cognitive levels fit awareness, training, and education. Questions are presented for further research as to unique designs and development of different security literacy programs.

Keywords: Bloom's Taxonomy, technical skills, computer security, training, education, higher education.

Recommended Citation: White, G., (2024). Higher Education Model for Security Literacy using Bloom's Revised Taxonomy. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.27-36.
<https://doi.org/10.62273/TRBS2965>

1. INTRODUCTION

The cyber security battle is being lost because *technology* is the focus of defense instead of the *people* who operate the computers (Jacobson, et al., 2012). "Often, organizations and countries invest in the technologies, forgetting that it is impossible to assure information security without raising awareness among users" (Ismailova, et al., 2019). Technology alone cannot shield computer systems from threats (Rhee et al., 2012). In today's world of computing, everyone is a target (Idziorek, et al., 2011). As Rhee et al. (2012) indicated, since technology alone cannot protect data and information systems from potential threats, there should be more effort made in addressing the human dimensions of information security (Rhee et al., 2012).

The information security field requires standardized education. (Spruit, 2022). The question is how to develop a standardized education that meets the needs of the security profession. There is little agreement about the competences with respect to information security that should be taught to meet the needs of the security profession (Bishop et al., 2017; Butler et al., 2018; Parker and Brown, 2019). This paper presents a framework of education in security literacy for higher education based on Bloom's Taxonomy.

To address the different characteristics of users this paper relates the three types of security literacy (awareness, training, education) with the different levels of cognition as defined by Bloom's Revised Taxonomy, and then focuses on which security literacy content best fits different postsecondary degree levels. Using this model of security structure will better address academic security literacy programs and curriculum needs.

2. LITERATURE REVIEW

Organizations should focus their security efforts equally on people *and* technology (Hewitt & White, 2020). Every person heading into the workforce needs to be educated about cyber security (Harris & Patten, 2015). Unfortunately, employees and employers fail to see security as a people issue (Ayyagari, 2012; Bulgurcu, et al., 2010; Kirkpatrick, 2006; Rezui & Marks, 2008).

"People are a crucial factor in ensuring the security of computer systems and valuable information resources" (Nieles, et al., 2017). People are fallible and are the weakest link in securing information systems (Caldwell, 2012; Ismailova, et al., 2019; Kirkpatrick, 2006;

Mitnick, 2002; Nieles, et al., 2017; Thomason, 2013). Studies have shown 95% of cyber security issues can be traced to human error (Mee & Brandenburg, 2020). "Each day, people are inundated with alerts and pop-ups informing them about patch updates, antivirus signatures, firewall exceptions, suspicious emails, and malware threats. These notifications fail to educate the user on how to make value-based decisions regarding the benefits and consequences of taking specific action on these items" (Security Literacy, 2022)

Security issues are people issues (Rezu & Marks, 2008). Yet people can be the first line of defense, first to detect and respond when an attack occurs. However, past research has focused on protective behavior rather than detection and response (Britt, 2008; Claar & Johnson, 2012; McLaughlin, 2006; Mensch & Wilkie, 2011; Pollitt, 2005; Puhakainen & Siponen, 2010; Wagley, 2010).

Since people are a primary target, education is one of the "secret weapons" in the cyber security battlefield. Further, if everyday users are the targets, then all audiences, not just technical and professional staff, need training and education in cyber security basics (Jacobson, et al., 2012). There is a need for users and professionals to learn information security. To get users to "think security" is to create a culture of security (Haber, 2009). Hence, information security literacy is needed (Piazza, 2006) and is an important defense (Jacobson, et al., 2012). "Just as drivers and passengers are taught how to wear seatbelts and to follow the rules of the road, citizens should be taught how to safely navigate the internet highway" (Mee & Brandenburg, 2020).

Computer security education is the key to combating the risks and vulnerabilities of information systems (Jacobson, et al., 2012). In the past, cyber security education was only a concern for computer and Internet experts (Idziorek, et al., 2011). "Universities have introduced technical degree programs in cyber security to meet industry demand for graduates with specialized skills" (Frydenberg & Lorenz, 2020). What a formal pedagogical approach to practical computer security education provides is the context and knowledge for students to apply computer security best practices before a cyber-attack. Then when faced with a critical situation, the user can be proactive rather than reactive in the face of new threats (Jacobson, et al., 2012). Applying countermeasures after an attack is too late (White, 2021).

"Most governments' strategies to improve cyber security overlook the importance of continued cyber risk education for its citizens across all ages and social demographics" (Mee & Brandenburg, 2020). Security education should not only prepare security professionals and IT technicians but the average end-user as well. Security literacy is for everyone.

However, one size does not fit all. Education programs need to be customized according to the needs of specific user groups (Bauer, et al., 2017). Harris & Patten (2015) used Bloom's Taxonomy to identify specific learning outcomes for courses in Information Technology curricula (Harris & Patten, 2015).

3. BLOOM'S REVISED TAXONOMY¹

In 1956 Benjamin Bloom and co-authors developed a classification of learning levels known as Bloom's Taxonomy. In 2001, the Taxonomy was updated to reflect 21st century educational goals (Anderson & Krathwohl, 2001; Krathwohl, 2002). This revised Taxonomy was used because of the different levels and types of cognition that were outlined in the paper. The levels are interdependent: Progress requires the ability to master the lower levels first.

"The interdependence of Bloom's different learning levels can be articulated through logic:

- Before we can understand a concept, we must be able to remember it.
- Before we can apply the concept, we must be able to understand it.
- Before we analyze it, we must be able to apply it.
- Before we can evaluate its impact, we must have analyzed it.
- Before we can create something based on the concept, we must have remembered, understood, applied, analyzed and evaluated the concept" (McNulty, 2019)

Subsequently, learning can move back and forth between the different levels depending on the learning situation. What follows is a brief synopsis of the six cognitive levels of Bloom's Revised Taxonomy, known as an "Education Framework" by McNulty (2019).

1. Remembering - Verbs: Describe, Identify, Label, List, Name, Recite, Repeat.

"Remembering is the act of retrieving knowledge and can be used to produce things like definitions or lists. It is the lowest of the taxonomic levels but is essential for the learning process because learners need to have knowledge in place before they can engage with it at higher cognitive levels. . . Remembering requires no understanding of the knowledge, only to have it accurately and thoroughly in mind." (McNulty, 2019).

2. Understanding - Verbs: Examine, Generalize, Group, Order, Paraphrase, Rephrase, Sort.

"The next level in the taxonomic structure is Understanding, which is defined as the construction of meaning and the building of relationships." (McNulty, 2019).

3. Applying - Verbs: Compute, Demonstrate, Direct, Dramatize, Formulate, Make, Present.

"The third level in Bloom's taxonomy, Applying, marks a fundamental shift from the pre-Bloom's learning era because it involves remembering what has been learnt, having a good understanding of the knowledge, and then being able to apply it to real-world exercises, challenges or situations." (McNulty, 2019).

4. Analyzing - Verbs: Simplify, Criticize, Distinguish, Explain, Illustrate, Inspect, Question.

"Analyzing is the cognitive level where a learner can take the knowledge they have remembered, understood and applied, then delve into that knowledge to make associations, discernments or comparisons. Analyzing would mean a learner can take complex information and simplify it or summarize it . . . or critically examine aspects of Bloom's original taxonomy and explain why his students later updated them." (McNulty, 2019).

5. Evaluating - Verbs: Decide, Forecast, Judge, Prioritize, Revise, Value, Weigh.

"The fifth level in Bloom's Digital Taxonomy is evaluation. This level requires the learner to make criteria-based judgements through the processes of critiquing and checking. Evaluating could involve reading a book and writing a review on its merits . . . suggesting ways to introduce digital technology into the classroom environment." (McNulty, 2019).

6. Creating - Verbs: Construct, Write, Develop, Design, Invent, Originate, Set up.

"The final taxonomic level is concerned with taking various elements and creating a new, coherent product. This level draws on all the other levels, with the learner remembering, understanding and applying knowledge; analyzing and evaluating outcomes and processes, and then constructing the end product, which may be either physical or conceptual. For example, . . . designing a 3D model of a house on a computer would both be examples of Creating. Another example would be a Learner taking the knowledge of Bloom's taxonomy which they have remembered, understood, applied, analyzed and evaluated, and creating a brand new model for the tiers of cognitive thinking and learning." (McNulty, 2019).

4. SECURITY LITERACY BASED ON BLOOM'S TAXONOMY¹

"The prime goal of practical computer security literacy is to provide students with security context for many of the activities they encounter throughout their everyday use of computers and the Internet. As a result, the topics and objectives of the corresponding modules are designed specifically to meet this goal and presented in a tangible format for students of all backgrounds to learn" (Security Literacy, 2022).

Security literacy is a combination of awareness, knowledge, and skills (Tills, 2017). "Starting with **awareness**, it builds to **training**, which evolves into **education**" (Wilson, et al., 1998). This flow moves people to higher cognitive levels. A Comparative Framework for awareness, training, and education is contained in NIST SP 800-27 Handbook, authored by Nieves, et al. (2017). See Table 1.

Awareness with Bloom's Taxonomy: Remembering, Understanding (what)

The first component of security literacy is an accurate and well-informed awareness of security issues (Tills, 2017). This involves the *recall* (remembering) of definitions and *concepts* along with the meaning and relationships (understanding) of these issues (McNulty, 2019). Cyber security awareness builds on basic information technology concepts (Frydenberg & Lorenz, 2020). And awareness reminds users of these issues and security practices to avoid failure, such as logging off a computer system or

locking doors (Nieves, et al., 202). Awareness deals with what is remembered and what concepts are understood.

From Bloom's Taxonomy perspective, the foremost course objective is for all the students to exhibit knowledge of practical computer security. In this context, knowledge is defined as student's ability to *recall* definitions of specific keywords (e.g., virus, phishing, keylogger), describe fundamental *concepts* (e.g., defense-in-depth, social engineering, security vs. privacy) and state computer security best practices (Idziorek, et al., 2011).

Training with Bloom's Taxonomy: Apply, Analyze (how to)

"The purpose of training is to teach people the skills (how to do it) that will enable them to perform their jobs more securely" (Nieves, et al., 202). Training provides the skills and abilities specific to an individual's roles and responsibilities relative to information security (Wilson, et al., 1998).

Skills training is learning how to apply knowledge and how to compare and summarize what is remembered and understood. A person must have this knowledge before applying it to new challenges or new situations. Teaching skills, such as understanding how data is gathered and how a digital identity is tracked online, can dramatically improve cyber security and the safety of a nation's citizens (Mee & Brandenburg, 2020). For example, a person who learns privacy skills will lead them to manipulate their privacy settings effectively, thus regulating the amount of their personal information that's exposed. Effective use of privacy settings after training can be a skill for security literacy (Tills, 2017).

Education with Bloom's Taxonomy: Evaluate, Create (why)

"Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security" (Nieves, et al., 202). This includes knowledge of laws, policies, and institutional practices and other concepts external to Information Security. Knowledge of technology resources to guide security behavior is also included in education (Tills, 2017). Education focuses on developing the ability and vision to perform complex multi-disciplinary activities and the skills needed to keep pace with threat and technology changes (Wilson, et al., 1998). With this in-depth and external knowledge, professionals are better able to *evaluate* the *whys* of security breaches and *create* countermeasures

and solutions that will protect data and systems in the event of a cyberattack.

From Harris & Patten (2015), examples showing associations with Literacy and Bloom's Levels are shown in Figure 1.

Figure 1. Three Literacy Types and Bloom's Taxonomy Levels (Harris & Patten, 2015)

Literacy	Bloom's	Outcomes	Examples
Awareness	Remember	- recall	Discuss user passwords. -recognize a phishing e-mail
Awareness	Understand	- meaning	Explain auditing. -know what a phishing e-mail can do
Train Skill	Apply	- new situation	Use access control in scenarios. -delete and report phishing e-mail.
Train Skill	Analyzing	- break into parts	Qualitative risk analysis. -determine phishing e-mail's characteristics
Educate	Evaluate	- judgments	Evaluate threats based on risk. -decide if e-mail is phishing and decide what to do.

5. HIGHER EDUCATION LEVELS BASED ON FIVE COMPETENCE LEVELS

Competence is the ability to apply knowledge, skills and attitude for achieving observable results (CEN, 2014). A competence statement of the required knowledge and skills. Spruit & van Noord (2014) developed five competence levels. See List 1. In Table 3, these competence levels are associated with Security Literacy categories to further show the progressing competencies.

Competence Levels 1 and 2 involve Bloom's remembering and understanding. They fit well with an Associate degree. Spruit (2022) describes Level 3 for a Bachelor's degree that stresses information security analysis of critical assets and implementing (apply) recovery plans. This level deals with Bloom's apply and analyze thinking skills. Spruit (2022) also describes Level 4 for a Master's degree that stresses technical research, design (create), execute a scientific research project and formulate conclusions. This level deals with Bloom's evaluation and creates thinking skills. Level 5 is an advanced version of Level 4.

List a: Competence levels 1 to 5 & Knowledge Skills by Spruit & van Noord (2014).

1. Basic knowledge and understanding of the subject. Carrying out the activity in a simple context.
2. Knowledge and understanding of all major aspects of the subject. Carrying out the activity in a simple context.
3. Knowledge and understanding of the subject in detail. Carrying out the activity in a difficult context.
4. Very extensive and detailed knowledge and understanding of the subject. Carrying out the activity in a very complex context.
5. Exceptionally comprehensive and detailed knowledge and understanding of the subject. Guiding others who carry out the activity in a very complex context.

6. HIGHER EDUCATION LEVELS BASED ON SEVEN INFORMATION SYSTEMS COMPONENTS²

Information security can be viewed as being different, at the varying levels of postsecondary education through seven components of information security. The seven components are *people, security, processes, technology, policies, standards, and procedures* (Rangaswami, 2005; Merkow & Breithaupt, 2006. p 70-74). These seven information security components best summarize the three higher education levels of security literacy curriculum.

Master's degree:

A Master's degree is people and policy focused and prepares future managers. Education at this level should involve the why's of security *policies*, dealing with *people* issues, and evaluation of threats and risks. (White, 2009). People with a Master's level education should be able to **create** security policies, to **evaluate** internal and external issues, and to **understand** the "why," when making decisions. This is what security professionals do.

Bachelor's degree:

A Bachelor's degree teaches *how* the security systems are developed and implemented to meet policy requirements. (White, 2009). Instruction should focus on *processes* and *standards* for development of security systems. When completed, a bachelor's candidate should know *how* to **analyze** security problems, and *how* to **apply** solutions and standards. This is what security managers do.

Associate degree:

An Associate degree curriculum should teach which security procedures and practices are to be maintained and monitored. (White, 2009). The curriculum should focus on the *technologies* and *procedures* to maintain and monitor data and systems. A person with an associate degree should **remember** and **understand** what to do to maintain and monitor operational security. This is what security technicians do.

6. HIGHER EDUCATION LEVELS BASED ON THREE SECURITY LITERACY TYPES AND BLOOM'S TAXONOMY²

Master's degree:

Why do security problems exist? This question of security leads to creating security policies that deal with people issues and evaluating internal and external risks. Creation of enterprise security architecture requires a common vision shared by planners, constructors, and administrators. It integrates management processes and policies for enterprise information security (Kim & Leem, 2005). The security professional must be able to evaluate needs to make security decisions.

Information security is a multi-disciplined subject. A security professional requires a wide range of backgrounds such as top-level management knowledge, external knowledge of laws, and awareness of social issues and trends. Security professionals must be educated in business functions such as accounting, finance, marketing, and management to better understand information security in a holistic business context (Rainer et. al., 2007). Along with core computer courses, other liberal arts studies are also needed because information security requires perspective of the environment computer systems work within to understand the whys. A wide range of educational experiences provides a good foundation for a career in Information Security. (Merkow & Breithaupt, 2006, p 7-8). Three universities Master's degrees stress critical thinking, strategic thinking, decision making, and research (ASU, 2023; Bellevue, 2023; ERAU, 2023).

Bachelor's degree:

How are security problems mitigated? This question of security involves **how** the security systems are developed and implemented to satisfy policies. Activities include planning, designing, establishing standards, and implementing security tasks. These activities included defining tasks and responsibilities of personnel, determining how information needs are related to tasks, how information is shared,

and the identification, valuation and classification of data assets (Kim & Leem, 2005; Steinke, 1997; Whitman & Mattord, 2005, p. 186). The training aspect of information security can be viewed as how to develop and **apply** security standards and effective security management practices (Whitman & Mattord, 2005, p. 187).

Required skills for such a security curriculum are problem solving (**analyze**), project management, risk management and technical skills (Armstrong & Jayaratna, 2002). Three universities describe their Bachelor's degrees as risk "analysis" and "applying" analytical tools to contemporary security (OU, 2023) as well as concepts and applications of information systems and technology in organizations (TSU, 2023). A Bachelor's degree stresses detect, manage, and prevent cyber-attacks (CIAT, 2023). Such undergraduate security courses provide a balance between theory and practice (Hsu & Backhouse, 2002).

By applying these skills, confidence and accountability are assured, and compliance with regulatory and legal requirements is provided. Risks are then lowered, control increases, and usable information is made available. These tactical benefits have a positive impact on an organization's relationship with its partners (Ezingear et al, 2004).

Pending on the nature of the subject of the Bachelor's degree, it can be considered either Training for technical subjects (no theory) or education when considering theory.

Associate degree:

What security procedures and practices are to be utilized? This question of security requires remembering procedures and involves an understanding of what practices should be utilized in any given situation. These procedures lead to successful daily maintenance and monitoring of technology and information and the enforcement of information security policies. (White, 2009).

These operation security procedures provide business continuity, secure and reliable access to information. The integrity and availability of an organization's data and systems are assured. Strict control procedures stop unauthorized access or software use in daily operations, and business processes and customer service improve. (Ezingear et al, 2004). Four colleges describe their Associate's degrees as acquiring "fundamental" working knowledge and technical skills in cyber security (CIAT, 2023; UST, 2023; CCIS, 2023; DeVry, 2023). Courses at this degree

level are technical and vendor specific and focus on the operational aspects of a business.

7. SUMMARY: EXAMPLES AND SUGGESTIONS

Because security literacy is different at the different levels of higher education, ascertaining the educational needs of students can become easier. Also, information security educators must be aware of current issues in the information security field to create curriculums that deal with a variety of current security issues. Using the new comparative framework of awareness, training and education helps instructors and administrators gain better insight into security literacy in higher education. (Surendran et. al., 2002).

As shown by Figure 2, higher education can be divided into three categories. These categories focus on different and progressive levels of thinking and competencies. This provides better insight into the development of college degrees.

Figure 2. Comparative Framework for Higher Education with Bloom’s Taxonomy and Security Literacy.

NIST SP 800:	Awareness	Training	Education
Attribute:	What is	How to	Why – reasons
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Bloom’s Taxonomy:	1. Remember 2. Understand	3. Apply 4. Analyze	5. Evaluate 6. Create
Higher Education:	Associate	Associate Bachelor	Bachelor Master

8. FUTURE QUESTIONS TO RESEARCH¹

Here are four questions for further research from Tills (2017) that can lead to the development of a variety of security literacy curricula (Tills, 2017). Bloom’s Taxonomy provides better understanding and insight to answer these questions.

1. What are the issues people need to be aware of for security literacy? (Tills, 2017).
2. Should there be multiple standards of security literacy (e.g., do some people need more advanced security training?)? (Tills, 2017). In other words, consider the different levels of thinking and cognition and the different characteristics of higher education degrees.

3. What is the minimum level of security awareness needed? (Tills, 2017). For example, recognizing an attack, i.e., phishing e-mail.
4. When should security literacy be more focused on awareness, rather than skills? (Tills, 2017).

Other questions: Are there limits for different people when it comes to Bloom’s Taxonomy of thinking and Spruit’s companies? Do some people function only at the lower thinking levels while others can progress to higher thinking levels? Do some people excel in security management issues while others can excel in security technology?

9. FUTURE RESEARCH

White (2009) authored a paper showing a model relating management levels and security needs. A future research paper could be the merging of the two models: Security Literacy and Bloom’s Taxonomy with different management levels’ security needs. A research question: What are the Bloom’s Taxonomy levels and Security Literacy levels associated with operational, tactical, and strategic management levels?

Here are two other possible future research projects: 1) Empirical research on three-degree type (AA, BA, MA) competencies and see how well they align with Bloom’s Taxonomy. 2) To determine if some students have limits as to how far they can progress up Bloom’s Taxonomy. Such findings can provide guidance as to what areas of security best fit them. Are high level thinkers best for security technology while low level thinkers are best for security management?

10. ENDNOTES

1. Parts of this paper came from a conference submission - White, G. (2022). "Security Literacy & Bloom’s Taxonomy." ISECON 2023, March 30-April 1, 2023, Plano, Texas.
2. Parts of this paper came from a journal paper – White, G. (2009). Strategic, Tactical, & Operational Management security model. *Journal of Computer Information Systems*, 49:3, 71-75, DOI:10.1080/08874417.2009.11645326. To link to this article: <https://doi.org/10.1080/08874417.2009.11645326>

11. REFERENCES

Anderson, L. & Krathwohl, D. (Eds.) (2001). A Taxonomy for Learning, Teaching, and

- Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Boston: Allyn & Bacon, Pearson Education Group.
- Armstrong, H. & Jayaratna, N. (2002). "Internet Security Management: A Joint Postgraduate Curriculum Design." *Journal of Information Systems Education*, 13(3), 249-258.
- Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, 8(2), 33-56.
- Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, 145-159.
- Bloom, B. & Krathwohl, D. (1956). Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. New York: Longmans, Green.
- Britt P. (2008). You've got mail...and security breaches. *Inf Today* 25(7), 1-1, 44.
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.
- Caldwell, T. (2012). Training – The Weakest Link. *Computer Fraud & Security*, 2012(9), 8-14.
- Claar C.L. & Johnson J. (2012). Analyzing home PC security adoption behavior. *J Comput Inf Syst.* 52(4), 20-29.
- Ezingear, J.N. & McFadzean, E. & Birchall, D. (2004). Board of Directors and Information Security: A Perception Grid. Paper No. 222 in Proceedings of British Academy of Management Conference, Harrogate.
- Frydenberg, M., & Lorenz, B. (2020). Lizards in the Street! Introducing Cybersecurity Awareness in a Digital Literacy Context. *Information Systems Education Journal*, 18(4), 33-45.
- Haber, L. (Apr 2009). SECURITY TRAINING 101. *Network World*, 26(16), 30, 32-33.
- Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. *Journal of Information Systems Education*, 26(3), 219-234. <https://libproxy.txstate.edu/login?url=https://www.proquest.com/scholarly-journals/using-blooms-webbs-taxonomies-integrate-emerging/docview/1810013990/se-2?accountid=5683>
- Hewitt, B. A., & White, G. (2020). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *Journal of Computer Information Systems*. On-line access: <https://www.tandfonline.com/doi/abs/10.1080/08874417.2019.1697860?journalCode=ucis20>. DOI: 10.1080/08874417.2019.1697860.
- Idziorek, J., Tannian, M., Jacobson, D., & Jacobson, D. (2011). TEACHING COMPUTER SECURITY LITERACY TO STUDENTS FROM NON-COMPUTING DISCIPLINES. *American Society for Engineering Education*. AC 2011-600.
- Ismailova, R. & Muhametjanova, G. & Medeni, T. D. & Medeni, I. T. & Soyly, D. & et al. (2019). Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. *Information Security Journal*, 28(4-5), 1Puhakainen & Siponen, 2010). -135. DOI:10.1080/19393555.2019.1685142
- Jacobson, D. & Rursch, J. & Idziorek, J. (2012). "Workshop: Teaching computer security literacy to the masses: A practical approach," 2012 Frontiers in Education Conference Proceedings, 2012, pp. 1-2, doi: 10.1109/FIE.2012.6462423.
- Kim, S. & Leem, C. S. (2005). Enterprise security architecture in business convergence environments. *Industrial Management + Data Systems*, 105(7), 919-936.
- Kirkpatrick, J. (2006). Protect your business against dangerous information leaks. *Machine Design*, 78(3), 66.
- Krathwohl, D. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice*, 41(4), 212-218.
- McLaughlin K. (2006). COMPTIA: end-user training is critical to security. *CRN* 1194, 35.

- McNulty, N. (2019). Everything you've ever wanted to know about Bloom's Taxonomy. Niall McNulty - Learning by Design, April 19, 2022. <https://www.niallmcnulty.com/2019/12/introduction-to-blooms-taxonomy/#:~:text=Bloom's%20Taxonomy%20provides%20a%20learning,%2C%20analysing%2C%20evaluating%20and%20creating> (accessed 6/16/2022).
- Mee, P. & Brandenburg, R. (17 Dec 2020). After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk. *World Economic Forum*. Geneva, Switzerland. <https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/> (accessed 5/Puhakainen & Siponen, 2010). /2022).
- Mensch, S. & Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Acad Inf Manage Sci J*. 14(2), 91-116.
- Merkow, M. & Breithaupt, J. (2006). *Information Security: Principles and Practices*. Pearson/Prentice Hall, Upper Saddle River, NJ.
- Mitnick, K. (2002). *The Art of Deception*. John Wiley & sons, Hoboken, NJ. (p. 3).
- Nieles, M., Dempsey, K., & Pillitteri, V.Y. (2017). SP 800-12: An Introduction to Computer Security: The NIST Handbook, Chapter 13. Computer Security Division-Computer Security Resource Center, NIST, Department of Commerce. <https://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter13.html> (accessed 5/30/2022).
- Piazza, P. (2006). Security goes to school. *Security Management*, 50(12), 46.
- Pollitt D. (2005). Energis trains employees and customers in IT security. *Hum Res Manage Digest*. 13(2), 25-28.
- Puhakainen P, & Siponen M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quart*. 34(4), 757.
- Rainer, R. K. & Marshall, T. E., & Knapp, K. J., & Montgomery, G. H. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? *Information Systems Security*, 16(2), 100-108.
- Rangaswami, M. R. (Feb, 2005). Finding Security. *Optimize*, 4(2), 67-68.
- Rezui, Y. & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27 (7/8), 241.
- Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.
- Security Literacy. Partnership for a Healthy Iowa. <https://ahealthyiowa.org/programs/security-literacy/> (accessed 5 29 2022).
- Surendran, K. & Ki-Yoon, K. & Harris, A. (2002). "Accommodating Information Security in our Curricula." *Journal of Information Systems Education*, 13(3), 173-176.
- Thomason, S. (2013). People - The Weak Link in Security. *The Global Journal of Computer Science & Technology*, 13(11), 6-12.
- Tills, C. (Aug 16, 2017). Security Literacy? Clear Security Communication. <https://www.clairtills.com/post/2017/08/16/security-literacy> (accessed 5 29 2022)
- Wagley J. (2010). Breaches lead to employee training. *Secur Manage*; 54(4), 44.
- White, G. (2009) Strategic, Tactical, & Operational Management Security Model. *Journal of Computer Information Systems*, 49:3, 71-75, DOI: 10.1080/08874417.2009.11645326. To link to this article: <https://doi.org/10.1080/08874417.2009.11645326>
- White, G. (2021). Generation Z: Cyber-attack Awareness Training Effectiveness. *Journal of Computer Information Systems*, 62(3), 560-571. DOI: 10.1080/08874417.2020.1864680.
- Wilson, M., de Zafra, D.E., Pitcher, S. I., Tiressler, J.D., Ippolito, J.B. (1998). NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST, Department of Commerce. <https://nvlpubs.nist.gov/>

nistpubs/legacy/sp/nistspecialpublication800-16.pdf (accessed 5/30/2022).

Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona

Paul Wagner
paulewagner@arizona.edu

Dalal Alharthi
dalharthi@arizona.edu

Department Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona 85747, USA

Abstract

Educating the next generation of cybersecurity professionals requires a shift into the K-12 space. Introducing cybersecurity at K-12 provides general cybersecurity literacy, career readiness, and early development of cybersecurity knowledge, skills, and abilities to become cybersecurity professionals. Cybersecurity education standards and guidelines traditionally focused on post-secondary education until 2021 when Cyber.org and TeachCyber released their K-12 Cybersecurity Learning Standards and the High School Cybersecurity Curriculum Guidelines respectively. Despite these initiatives, there is limited literature on the development of cybersecurity programs at secondary education institutions. Also, available resources to develop and support these programs differ from district to district and among states. To overcome these deficits, this paper presents a case study conducted at a comprehensive four-year cybersecurity program at a secondary education institution. The case study consisted of open-source research, document reviews, questionnaires, and interviews. The data collected were compiled into a program profile consisting of student enrollment; demographics; personnel; operational requirements; formal, informal, and non-formal learning activities; and pathway opportunities. The developed program profile provides a structure to analyze other programs internal or external to Arizona. The enhanced data set can provide the ability to compare programs to develop best practices for establishing cybersecurity education programs at secondary education institutions. This profile can allow schools considering the development of a program at their institutions to better understand the requirements and resources needed to establish the program. Additionally, the data collected provides a baseline to compare their district and school to understand the implications within the context of their environment.

Keywords: Cybersecurity Education, Workforce Development, K-12 Education, Program Evaluation, Educational Strategies

Recommended Citation: Wagner, P., Alharthi, D., (2024). Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.37-63.
<https://doi.org/10.62273/HVQA9947>

1. INTRODUCTION

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. The most recent (ISC)2 Cybersecurity Workforce Study estimates a global cybersecurity workforce gap of over 3.4 million (ISC2, 2022). CyberSeek estimates that there are over 750,000 cybersecurity job openings (CyberSeek, 2023). As cybersecurity threats continue to grow in sophistication, scope, and scale, the ability to secure the United States from these threats lies in the ability to develop cybersecurity professionals with the Knowledge, Skills, and Abilities (KSAs) to accomplish the tasks associated with cyber roles. The ability to supply qualified cybersecurity professionals is outpaced by the growing demand as previously outlined. Cybersecurity programs have been expanding at post-secondary institutions and are being introduced at secondary education institutions. This paper reviews a case study conducted on an established four-year comprehensive cybersecurity program at a secondary education institution in Arizona.

2. LITERATURE REVIEW

A Systematic Literature Review (SLR) technique was used to find relevant articles from 2010 to 2023. Selected articles provided relevant information for analysis and discussion, covering topics such as cybersecurity, standards, guidelines, education, K-12 education, legislation, dual enrollment, certifications, and safety. Given the limited research on K-12 cybersecurity education and its relevance to current workforce shortages, a comprehensive set of search criteria was employed. Full-text journal articles were analyzed to explore initiatives in K-12 cybersecurity education, training, and workforce development. Information from these articles was used to develop questionnaires, interview guides, and program profiles. Editorials, trade journals, and online resources were also consulted to gather current statistics, applications, and concerns in cybersecurity education and workforce development.

K-12 Education

At a fundamental level, cybersecurity education is, "providing students with an understanding of how connected electronic devices interact in a digital age, how to protect digital assets from vulnerabilities and the moral and ethical issues surrounding the uses of technology in our society." ("The State of Cybersecurity", 2020).

K-12 education institutions have a key role in addressing the cybersecurity professional shortage in two primary ways. First, K-12 education provides the ability to raise awareness and interest in cybersecurity careers. Second, it provides a conduit for fundamental knowledge needed to pursue post-secondary education or career pathways in this field. However, nationally there is a lack of quality Science, Technology, Engineering, and Math (STEM) programs, which cybersecurity is part of; lack of accessibility by all students, specifically minority students and students from lower Socio-Economic Status (SES); and overall stagnant performance in STEM assessments (Burke, 2021). Additionally, 75% of recent high school graduates feel they are underprepared to make college and career decisions (Lucariello, 2022) and are underprepared to enter the workforce (Lim, 2019). Further, the results of a 2020 national survey on the state of cybersecurity education in K-12 schools identified the following:

- Most K-12 educators do not know a lot about cybersecurity education.
- Cybersecurity deserts associated with inequitable access to cybersecurity education persist.
- Most students know little or nothing about cybersecurity.
- Access to cybersecurity education is infrequent and uneven.
- Cybersecurity education is rarely a focus of extracurriculars despite student interest.
- Cyberbullying and Terrorism are the most frequent cybersecurity education topics in K-12 schools ("The State of Cybersecurity", 2020).

Standards

There are multiple standards organizations aligned with cybersecurity workforce and education. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181 (Petersen, 2021), the National Security Agency's (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) (NCAEC, N.D.), the Association for Computing Machinery's (ACM) curriculum guidelines for post-secondary degree programs in cybersecurity ("Curriculum Guidelines", 2017) and cybersecurity curricular guidance for associate-degree programs ("Cybersecurity Curricular Guidance", 2020) provide guidance on cybersecurity curriculum mainly focused on post-secondary education.

K-12 specific cybersecurity education standards and guidelines were not available until 2021 when

the national K-12 Cybersecurity Learning Standards ("K-12 Cybersecurity Learning Standards", 2021) and the High School Cybersecurity Curriculum Guidelines (Dark, 2021) were released. The K-12 Cybersecurity Learning Standards identify key fundamentals of cybersecurity education including computing systems, digital citizenship, and security ("K-12 Cybersecurity Learning Standards", 2021). The Curriculum Guidelines identify eight "Big Ideas" which include ethics, establishing trust, ubiquitous connectivity, data security, system security, adversarial thinking, risk, and implications (Dark, 2021).

Curriculum

Similar to standards, there are multiple resources for cybersecurity education content developed for post-secondary. The National Cybersecurity Training and Education (NCyTE) ("Cybersecurity Curriculum," 2021), Centers of Academic Excellence in Cybersecurity Resource Directory (CARD) ("CARD," 2021), and Cybersecurity Labs and Resource Knowledgebase (CLARK) ("CLARK," 2021) provide various resources ranging from nanomodules (1 hour or less) to full courses (15 weeks) across a wide range of subjects.

Cyber.org and the RING (Regions Investing in the Next Generation) programs provide cybersecurity curricula specific to K-12. Cyber.org provides four cybersecurity-specific courses for K-12 education: Cyber Literacy (Grades 8 – 10), Cyber Literacy II (Grades 9 – 12), Cybersecurity Basics (Grades K – 8), and Cybersecurity (Grades 10 – 12) ("Cybersecurity," 2022).

RING is "an online high school cybersecurity course that offers interesting and engaging content specifically for students and schools without an existing cybersecurity program" that was officially launched in the summer of 2022 (Hairston, 2022). The program is divided into ten units consisting of an introduction, ethics, establishing trust, ubiquitous connectivity, data security, introduction to Python programming, system security, adversarial thinking, risk, and implications. RING is designed to be a fully developed year-long program for secondary education.

Despite the increasing amount of information on cybersecurity education, content, and curriculum, there is a lack of understanding of how cybersecurity education programs are developed, the resources needed to support these programs, and the formal, informal, and non-formal learning activities integrated into these programs.

3. RESEARCH METHODOLOGY

The purpose of this study was to identify the elements of a comprehensive high school cybersecurity program and develop a program profile containing the elements identified during research, document review, questionnaires, and interviews. The focus of the

Research Approach

This work utilized a case study approach. Yin (2003) defined a case study as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are evidence...and it relies on multiple sources." This research utilized multiple data collection techniques including reviewing relevant documents, conducting interviews, and compiling direct observations of the program.

Research Design

The five components related to case studies identified by Yin (2003) informed the research design and included the study's questions, study propositions, unit(s) of analysis, the logic linking the data to the propositions, and the criteria for interpreting findings.

Publicly accessible data was collected to establish the initial program profile. Questionnaires and interviews were conducted to identify additional elements missing from the initial program profile and provide context on how the program was established, identify the personnel and resources available, identify challenges and opportunities in establishing the program, and identify future growth and initiatives pursued by the programs.

The interviews followed a semi-structured approach where the interviewer and respondents engaged in a formal interview, the interviewer developed and used an interview guide, and although the interviewer followed the guide, topical trajectories which strayed from the interview guide were followed when appropriate.

Study propositions direct attention to something that should be examined in the scope of the study (Yin, 2003, p. 22). Based on the literature review about the current state of cybersecurity education institutions the following proposition was identified: Evaluating current cybersecurity programs at secondary education institutions can identify elements of a comprehensive cybersecurity education program.

The unit of analysis for a "case" study can be an individual, an event, or an entity. The unit of analysis for this case study was defined as the

cybersecurity education program at Basha High School located in the Chandler Unified School District in Chandler, Arizona. Basha High School's cybersecurity program was selected since it is the most comprehensive and established program within Arizona. Stakeholders were identified as those having direct involvement in developing the program and those who had secondary input or taught within the program. All data collected were used to develop the program profile and used to address the proposition.

Finally, analogic inference was used to interpret the findings since statistical analysis would not be appropriate due to the limited number of interviews conducted. Analogic reasoning provides the ability to determine similarities and to make inferences from one situation to another (Calhoun, 2009). This method was appropriate considering that secondary education institutions share a similar architecture, follow state testing standards, and generally follow similar operational aspects.

4. ANALYSIS AND RESULTS

Researchers identified the salient elements informed by the literature review and interviews conducted during this study. The elements identified were enrollment; demographics; operations which included personnel and equipment; formal, non-formal, and informal learning activities; and pathways. The program profile provides insight into the cybersecurity program at the secondary education institution within Chandler Unified School District. The insight can identify personnel, resources, challenges, and opportunities for other schools interested in understanding the requirements to develop cybersecurity education programs at their institutions.

Basha High School's Cybersecurity Program

The entirety of Basha High School's program profile can be found in Appendix A. This section highlights some of the important data collected at this school. The program began in the 2019-2020 school year with 60 students. The 2022-2023 school year had 154 students. Figure 1 depicts the student enrollment breakdown. The cybersecurity program graduated one student in 2020, one student in 2021, two students in 2022, and 17 students in 2023 (Figure 2).

The operational aspects of the cybersecurity program consist of personnel, equipment, network, and facilities. The program is primarily supported by three Full Time Equivalent (FTE) teachers. The itemized initial equipment list for

year one operations is in Appendix A. Initial startup costs were approximately \$32,000. Additionally, the program required a separate network from the school district-provided network. The isolated network was installed in the cybersecurity classrooms and lab spaces to allow access to websites and resources to facilitate learning objectives that would be blocked on the district network. This isolation also required separate hardware due to restrictions on district-provided equipment. Finally, the program has four dedicated learning areas. There are three general-purpose classrooms and one Career and Technical Education (CTE) lab. The CTE lab has a larger footprint consisting of teaching space and a space for hands-on activities and equipment storage.

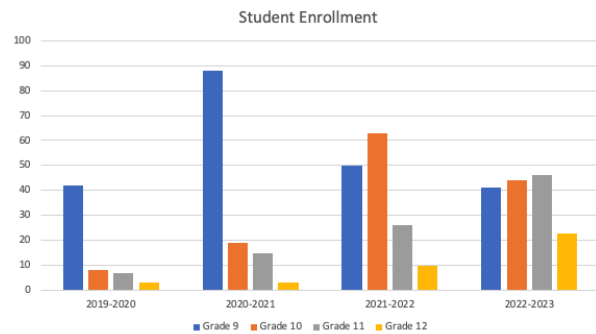


Figure 1: Basha High School Student Enrollment

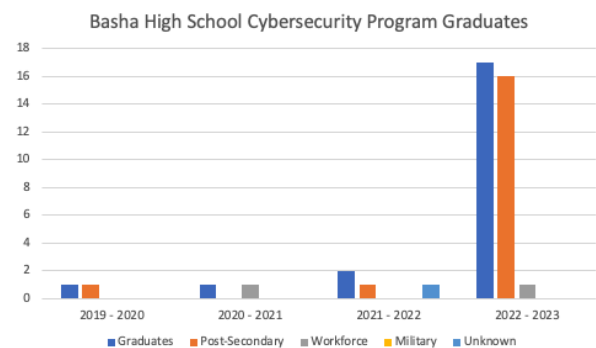


Figure 2: Basha High School Program Graduates

Basha High School's cybersecurity program's formal learning activities were modeled after the established pathway between Chandler Gilbert Community College (CGCC) and the University of Arizona (UA). Developing the program had an initial goal of providing a seamless pathway from the high school, through the community college, to the university. The courses within CGCC's cybersecurity program were analyzed to identify which courses would fit into Basha High School's cybersecurity program and articulation and

pathways for students, meet dual-enrollment requirements, and align with existing Arizona CTE technical standards for network security identified as 11.1999.00. Ten courses were identified for inclusion into the program: Introduction to Computer Systems, Hardware and Software Configuration and Support (A), Hardware and Software Configuration and Support (B), Introduction to LAN and Security Fundamentals (A), Introduction to LAN and Security Fundamentals (B), Linux OS, Advanced Linux, Information Security Fundamentals, Ethics in Information Technology, and Python. The descriptions for each course are outlined in the Basha High School cybersecurity program profile in Appendix A. Each of the ten courses allows dual enrollment.

Additionally, Basha High School is a Cisco Networking Academy (NetAcad). This provides access to curriculum and teaching resources, equipment and software, professional development opportunities, and help students access job opportunities (Cisco, 2023). Further, the program leverages content, assessments, and labs from Cisco, TestOut, and Cengage to meet formal learning objectives. The course alignments and costs of these materials are outlined in Appendix A. The program used RedHat Linux since program inception; however, due to changing requirements, the program will switch to Cisco curated content beginning in the 2023 – 2024 school year.

Non-formal learning activities include camps, certifications, internships, and externships. AZ Cyber Initiative and CyberPatriot are the cybersecurity-specific camps currently offered as part of Basha's cybersecurity program. AZ Cyber Initiative is a multifaceted program offering scholarships, mentorship, internships, and cybersecurity boot camps. Scholarships provide financial assistance for high school students pursuing degrees or professional certifications in cybersecurity-related fields or cybersecurity-related careers in the U.S. military. The mentorship program "connects high school students with qualified professionals to gain unique insights and important tools to help them find greater success ("AZ Cyber Mentorship", 2023)." Paid internship opportunities are provided to students who complete the associated boot camp which will be discussed next. These internship opportunities place students with companies and professionals to serve as cyber consultants for small businesses. Finally, AZ Cyber Initiative provides camps to high school students and teachers. Each boot camp is a weeklong course that provides students with

knowledge, hands-on activities, career development, and career exploration. The teacher boot camp prepares teachers to integrate content into existing courses and develop cybersecurity courses or programs.

The CyberPatriot program provides multiple resources for middle and high school students. Basha High School began offering CyberPatriot camps in August of 2022. CyberPatriot offers a standard camp consisting of an introduction to CyberPatriot, an introduction to virtual machines, cyber ethics, Windows 10 and Ubuntu 18 Operating Systems. Additionally, an advanced camp offers cyber ethics, Windows 10 and Ubuntu 18 Operating Systems focusing on advanced skills and system administrator tasks and provides Cisco NetAcad access. Both camps offer a competition day to compete against other camps nationally.

A detailed discussion of the certifications integrated into Basha High School's cybersecurity program is outside the scope of this study. Program curriculum aligns with or introduces concepts for CompTIA's A+, ITF+, Linux+, Security+, TestOut's Security Pro, and Python Institute's Python Certified Entry-Level Program (PCEP) certifications. Certification allows high school students to be more employable and validate a foundational level of proficiency in several IT and cybersecurity work roles. For example, A+ aligns with Information Assurance Technical (IAT) I and Security+ aligns with Information Assurance Manager (IAM) I Department of Defense (DoD) approved baseline certifications ("DoD Approved 8570 Baseline Certifications," 2023).

Basha High School has partnered with several partners to provide students the opportunity to participate in internships and externships. The partnership with Open Source Integrators allows students to work with teams of open source Enterprise Resource Planning (ERP) professionals. The partnership with ElevateEdAZ provides externship opportunities focused on aligning education to workforce learning paths. This initiative prepares students for college and careers by partnering with education, business, and the community. The program specifically focuses on creating opportunities for high-wage, high-demand pathways which include Information Technology and Cybersecurity. This externship provides participants with a stipend upon completion of the program. The weeklong externship program consists of multiple sessions on technology-related topics, career pathways, required skills, and current events. Additionally,

students participate in team-based projects and job preparation, and professional development sessions.

Informal learning activities include clubs, competitions, self-study and ad-hoc learning, conferences, and industry events. Basha High School's cybersecurity program integrates multiple informal learning activities for students. As part of their overall CTE program, The Future Business Leaders of America (FBLA) and Family, Career, and Community Leaders of America (FCCLA) prepare students to become community-minded business leaders. FCCLA is an example of a student club. Additionally, Basha High School's cybersecurity program offers students the opportunity to compete in the CyberPatriot competition and National Cyber League (NCL). CyberPatriot is typically held during the fall semester and NCL is held in the spring allowing students to compete throughout the school year. CyberPatriot competitions consist of a network security challenge and a Cisco networking challenge. Teams compete over six hours. Whereas CyberPatriot focuses on network defense, National Cyber League is a comprehensive competition including Open Source Intelligence (OSI), cryptography, password cracking, log analysis, network traffic analysis, forensics, web application exploitation, scanning, and enumeration and exploitation (NCL Categories, 2023). Additionally, the Basha cybersecurity program set up a tour of the PhoenixNAP Data Center providing insight into one aspect of the career field. Finally, self-study and ad-hoc learning and conferences are not coordinated through the program but advertised and encouraged. Teachers and students participated in CactusCon a Phoenix-based cybersecurity conference, Women in Cybersecurity (WiCyS), NICE K-12 Conference's student signing day, and Embry Riddle Aeronautical Engineering cyber day.

Pathways become part of a future-focused program. Preparing students for post-secondary education, trade schools and certification training, military service, or the workforce provide options and opportunities. As previously mentioned, the formal learning activities were designed with pathways in mind. Specifically, this is the partnership with CGCC and UA. These designed pathways do not limit student opportunities for other post-secondary opportunities. Alternatively, students can pursue certification and workforce opportunities through Advanced Business Learning (ABL). ABL is a state-licensed school providing concurrent, subsequent, or alternative learning paths to

develop cybersecurity knowledge and skills and obtain industry certifications. ABL provides cybersecurity-related training aligned with DoD 8140 requirements, access to a cyber practice range, Risk Management Framework (RMF), and certification training for A+, Network+, Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP). Basha's cybersecurity program partners with the school's Junior Reserve Officer Training Corps (JROTC) program. JROTC provides exposure to military service. Additionally, the school offers the Armed Services Vocational Aptitude Battery (ASVAB) to students during the fall semester. This provides the opportunity for career exploration and provides an initial starting point for enlisting in military service. Finally, as an anecdotal example of direct-to-workforce pathway options, one of the first program cohort graduates was offered employment with Kelly Technologies.

Interview Results and Analysis

Interviews were conducted with the cybersecurity program director and two teachers involved in program development. Study participants completed the questionnaires and answered interview questions outlined in Appendix B to identify programmatic elements, motivations, challenges, and opportunities in program development. This section presents the results from interviews conducted at Basha High School.

The primary motivation for developing the cybersecurity program was a school district initiative sparked by an administrator attending a cybersecurity conference at the University of Arizona (UA). The district administrator was presented with the pathway from CGCC to UA and decided to develop a dual enrollment pathway to CGCC from Basha High School. Basha High School was selected due to the available land and planned development of the building which now houses the Institute of Cyber Operations and Networking (ICON). The program director previously taught cybersecurity courses at another high school and was identified and eventually hired to establish the program at Basha High School. When asked about personal motivation to develop the program, the director stated:

"I attended a lot of conferences while preparing the course in cybersecurity. The cybersecurity community was welcoming, there wasn't competition among teachers and industry professionals, there was an obvious need for cybersecurity education, and I understood the importance. I took

the opportunity to make the biggest difference to the biggest number of students. Cybersecurity offers something for everybody.”

Cybersecurity standards, curricular guidelines, and frameworks did not exist when the Basha High School program was developed. The Technical Security Guidelines for Network Security 11.1999.00 CTE requirements were available; however, these were not used initially to develop the program. Despite this, the program must align to these standards which introduces some issues. Computer science, programming, and operating system courses are included in the program which adopts the Arizona Computer Science Standards from the Arizona Department of Education (ADE). Additionally, the program includes the ten dual enrollment courses outlined in the program profiles. The CTE and dual enrollment requirements create challenges as described by study participants:

“State ADE Computer Science Standards require approval to bring in additional curriculum. Getting resources and approvals for the curriculum is an administrative burden. For example, I put in a request in July 2022 and still waiting on approval in April 2023.”

“Have to follow specific requirements which reduce flexibility and technology changes too fast to follow these timelines.”

The operational elements include instructors, hiring challenges, equipment, networks, and facilities. Recruiting and retaining cybersecurity teachers is challenging. There may be teachers that are ineligible to be CTE-certified or dual enrollment certified in cybersecurity due to a lack of education or experience. Alternatively, industry professionals, people with the appropriate education without teaching experience, or individuals unwilling to teach due to the pay differential present additional challenges. Basha’s program has had challenges with hiring and retention. For example, one teacher quit within 30 days. This individual was an industry professional with experience teaching post-secondary students but not secondary education. The individual did not feel the opportunity was a fit. A qualified teacher from the community college worked at the high school on an interim basis due to a lack of qualified teachers within the cybersecurity program to teach required courses. Another teacher left for industry opportunities with higher salary. Finally, a teacher was relieved

of their duties for undisclosed reasons. This demonstrates rapid turnover over the four years of the program. Compounding this problem is that certifying teachers for CTE or dual enrollment can be lengthy. CTE certification requires classes on teaching, advisory board, and other requirements; state certification, and 140 hours of internship. This process typically takes six months. Alternatively, 5000 hours of industry experience can result in CTE credentialing. Each of these credentialing options represents a significant investment in time impeding the point-in-time need for teachers in the program. Dual enrollment certification is conducted by the community college and every community college has different certification requirements and processes. Specific comments from study participants included:

“Recruitment and Retention are challenges. Potential teachers don’t fit both molds of CTE and Dual Enrollment. May not be a fit for classroom requirements for secondary education and how to deal with “kids.””

“It was a long process to get dual enrollment certification and to introduce new courses.”

“Money is a barrier. Teaching is a profession that doesn’t yield the same results as industry.”

“Have to have a love for teaching and content expertise. You can write code and automate tasks that can do something repeatedly. Teaching is not like that, and every new year requires a teacher to do things manually over and over again.”

The program profiles outline specific equipment, networks, and facilities available to the programs and teachers. All study participants stated that they had the necessary networks and facilities to meet learning objectives and support the program. For equipment, the Technical Standards provided information aligned with the networking aspects but didn’t address cybersecurity holistically. The curriculum and courses dictated equipment requirements. Initial equipment requirements required research on setting up labs, furniture, and space. The school provides basic equipment for classroom instruction; however, the restrictions placed on the machines or their limited technical specifications hinder teaching certain content in the program. The following are study participant statements regarding networks and equipment:

"District machines do not support cybersecurity education. Had to beg for computers and equipment to support CyberPatriot and other activities. Requested CPU kits for students to build computers associated with A+ / Hardware courses. Everyone has the same equipment for these courses to facilitate teaching and learning."

"Convincing and justifying the need for equipment not on the pre-approved list was challenging."

"Have donated equipment but don't have the infrastructure to support the equipment. Power to support networking equipment is an example. Would like to set up a cyber or networking range but don't have the equipment or infrastructure to support it."

"District has certain restrictions which limit access to certain websites and software that can be loaded on machines. Impedes teaching certain material."

Formal learning activities were built based on the established pathway between CGCC and UA. Individual courses were developed to maintain dual enrollment requirements and the overall pathway. The course and course descriptions for these courses are outlined Appendix A. Additionally, Appendix A contains the specific non-formal and informal learning activities related to the cybersecurity programs. This section will address the perceived need to include non-formal and informal learning activities into the cybersecurity program. All study participants overwhelmingly agreed that non-formal and informal learning activities are critical to student learning and success. These opportunities provide alternate credentialing in the forms of certifications, experience from internships, and career exploration through externships and guest speakers. Additionally, competitions increase student engagement and understanding of the concepts covered in formal learning activities. Study participants provided the following responses specific to non-formal and informal learning activities:

"Certification is a requirement of CTE. The program must align to a certification. Avenues with each class so that students can seek out opportunities after any year in the program. Show students the options they have within the curriculum.

Stronger more comprehensive foundation."

"Camps provide the opportunity to work with other kids to develop skills different than course requirements. Builds comradery. Being around like-minded people. Introduces career exploration."

"Internships and Externships provide paid opportunities in high school. Working directly with the company. Students learned more about the requirements of the workplace. It is exciting and provides opportunities to gain industry experience. "Can't put a price tag on that experience.""

"Competitions provide a fun learning environment. Drives students to succeed and work as a team. Students are engaged in the process. Competitions make learning great by sharing and reviewing the information from competitions."

"CTFs, HackTheBox, and CyberPatriot activities keep student interest up. Helps keep students in the program."

"Activities like these enhance student engagement and allows them to make sense of where to apply the things they are learning in formal learning activities. The real world application of concepts."

The program has the articulated pathway to CGCC and then UA. Although this pathway was a primary driver for program development, the program is designed to provide opportunities for students to enter the workforce, join the military, seek certification training, or attend post-secondary education. The program uses an access database to track students throughout the program. All students are required to complete a program-developed exit survey which asks for personal email addresses and plans post-graduation. Additionally, all students are required to fill out a survey for CTE completion. These surveys are given to students during classroom time to obtain maximum participation. The four-year program provides a solid foundation to pursue cybersecurity-specific and non-cybersecurity opportunities after graduation. Survey participants provided the following responses regarding pathways:

"The four-year program provides a solid foundation. No matter where they are at

in their senior year they have multiple opportunities to choose the pathway. Comprehensive enough to have choices. Cuts down on entry time into the field based on their experience.”

“Hands-down prepares students with applicable information to succeed in fields outside cybersecurity-specific roles. Good employees with a foundation in technology and security. Provides different perspectives since people must interact with people in IT, Finance, and other business functions.”

“Good foundation for other STEM fields such as engineering, biomedical engineering, computer science, and other disciplines.”

“Industry engagement and building in activities into the program builds pathway opportunities for students. Provides tangible things to get students engaged in workforce opportunities.”

“Focus on analysis and problem solving skills that can be applied to other situations.”

“The comprehensive nature of the cybersecurity program can expose students to many different disciplines and if students lose interest in one area they can shift to another while still staying in STEM-related fields.”

Participants' responses provided valuable insights for program profiles and identified additional recommendations, opportunities, and challenges. Table 1 provides a breakdown of those responses.

<p>Recommendations</p>	<ul style="list-style-type: none"> • Infuse yourself into industry by attending conferences and events to get ideas from others. • Be creative and solve problems. • Educate and work with people around you.
<p>Opportunities</p>	<ul style="list-style-type: none"> • Cybersecurity programs provide pathways to high paying / high opportunity jobs. • The country has a dire need for

	<p>cybersecurity professionals.</p> <ul style="list-style-type: none"> • These programs can make students better employees and citizens. • Increased student enrollment attracting different student demographics to the school and program.
<p>Challenges</p>	<ul style="list-style-type: none"> • Cybersecurity programs are a new concept for schools and the state. Can be challenging to get buy-in for time and resources. • Need to get administration at the school and district level engaged and bought into the idea. • Should cybersecurity courses be considered “weighted courses”? • CTE requirements to pass certain industry certifications can be challenging. • School counselor engagement and focus to determine what is best for student instead of forcing them into traditional paradigms. Cybersecurity courses didn't exist years ago. • Priorities within school: foreign language vs CS courses. • Teachers responsible for marketing their own programs without marketing experience or resources.

Table 1: Recommendations, Challenges, and Opportunities

5. FUTURE WORK

This study provides multiple opportunities for future research. The program profile provides a baseline to begin discussions with other school districts within Arizona and beyond. Additional

program profiles could be developed at institutions across the country to develop a broader range of profiles. Additionally, interviews and focus groups could be conducted with different stakeholders to identify schools interested in developing cybersecurity education programs. Further, the scope of stakeholders could be expanded to include administrators, teachers, and staff involved in cybersecurity education or interested in supporting these programs.

6. CONCLUSIONS

Cybersecurity education and training initiatives continue to evolve in the United States. As K-12 institutions evaluate the potential introduction of cybersecurity content, curriculum, and programs, it is crucial to conduct a thorough assessment of the return on investment for pursuing these endeavors. This paper has presented a case study conducted on a four-year cybersecurity program at a secondary education institution in Arizona. The developed program profile provides a structure to analyze other programs internal or external to Arizona. By leveraging an enhanced data set, secondary schools considering the development of their own programs can gain a better understanding of the requirements and resources needed to establish successful initiatives. Additionally, the collected data can provide a baseline to compare their district and school to understand the implications within the context of their environment. Finally, the profiles identify existing opportunities for non-formal and informal cybersecurity learning activities to expose students to cybersecurity KSAs without building an entire program. This has far-reaching implications for the cybersecurity field and contributes to the broader student development within STEM disciplines.

7. REFERENCES

"AZ Cyber Initiative Mentorship Program," (2023). AZ Cyber Initiative. Retrieved June 3, 2023 from <https://azcyber.org/mentorship-program/>

Burke, A. and Rotermund, S. (2021). Elementary and Secondary STEM Education. National Science Foundation / National Science Board: Science and Engineering Indicators. <https://nces.nsf.gov/pubs/nsb2021/student-learning-in-mathematics-and-science>.

"Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," (2017). CSEC. Association for Computing Machinery. Retrieved June 3, 2023 from <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>.

"Cyber Literacy," (2019). Cyber Literacy 1. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from <https://cyber.instructure.com/courses/4>.

"Cyber Literacy II," (2019). Cyber Literacy 1. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from <https://cyber.instructure.com/courses/37>.

"Cybersecurity," (2022). Cybersecurity. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from <https://cyber.instructure.com/courses/100/p/ages/course-information>.

"Cybersecurity Basics," (2022). Cybersecurity Basics. Cyber Innovation Center and Cyber.org. Retrieved June 3, 2023 from <https://cyber.instructure.com/courses/227>.

"Cybersecurity Curricular Guidance for Associate-Degree Programs," (2020). CCEC. ACM Committee for Computing Education in Community Colleges. Retrieved Jun 3, 2023 from <http://ccecc.acm.org/files/publications/Cyber2yr2020.pdf>.

"Cybersecurity Curriculum," (2021). NCyTE Center. <https://www.ncyte.net/resources/cybersecurity-curriculum>.

"Cyberseek Cybersecurity Supply/Demand Heat Map," (2023). CyberSeek. Retrieved June 3, 2023 from <https://www.cyberseek.org/heatmap.html>

Dark, M., Daugherty, J., Emry, M., Masey, D., and Peyrot, J. (2021). High School Cybersecurity Curriculum Guidelines & Glossary. Teach Cyber. <https://teachcyber.org/wp-content/uploads/2021/04/High-School-Cybersecurity-Curriculum-Guidelines.pdf>.

"DoD Approved 8570 Baseline Certifications," (2023). DoD Cyber Exchange. <https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/>.

Hairston, J and Sands, J. (2022). RING (Regions Investing in the Next Generation). CAE in Cybersecurity Community. <https://caecommunity.org/initiative/k12-ring>.

"(ISC)2 Cybersecurity Workforce Study," (2022). (ISC)2. Retrieved June 3, 2023 from <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>.

Lim, V. (2019). Students don't feel their high schools prepare them for careers. Working Nation. <https://workingnation.com/prepare-ri-provides-experiential-learning-students/>.

Lucariello, K. (2022). National Survey Finds High School Graduates Not Prepared for College or Career Decisions. The Journal: Transferring Education Through Technology. <https://thejournal.com/articles/2022/12/05/national-survey-finds-high-school->

graduates-not-prepared-for-college-or-career-decisions.aspx.

"National Centers for Academic Excellence in Cybersecurity," (N.D.). National Security Agency / Central Security Service. Retrieved June 3, 2023 from <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/>.

Petersen, R., Santos, D., Smith, M., Wetzel, K., and Witte, G. (2020). NIST Special Publication 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework). National Institute for Standards

and Technology.
<https://doi.org/10.6028/NIST.SP.800-181r1>.

"The State of Cybersecurity Education in K-12 Schools," (2020). EdWeek Research Center Cyber.org. Retrieved June 3, 2023 from <https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf>.

Yin, R. K. (2003). Case study research: Design and methods (3rd edition). Thousand Oaks, CA: Sage Publications.

Editor's Note:

This paper was selected for inclusion in the journal as an ISCAP Cybersecurity 2023 Distinguished Paper. The acceptance rate is typically 7% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2023.

Appendix A: Basha High School Program Profile

Enrollment

Academic Year	Grade 9	Grade 10	Grade 11	Grade 12	Total	Graduates
2022 - 2023	41	44	46	23	154	17
2021 - 2022	50	63	26	10	149	2
2020 - 2021	88	19	15	3	125	1
2019 - 2020	42	8	7	3	60	1

2022 - 2023 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	41				41
10th	20	24			44
11th	11	5	26	4	46
12th	6	4	1	12	23
Total	78	33	27	16	154

* Year 3 Students are taking Year 3 and Year 4 courses.

2021 - 2022 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	50				50
10th	25	38			63
11th	11	3	12		26
12th	6	3	1		10
Total	92	44	13		149

2020 - 2021 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	59	29			88
10th	18	1			19
11th	12	3			15
12th	2	1			3
Total	91	34			125

2019 - 2020 School Year					
Grade Level	Year 1	Year 2	Year 3	Year 4	Total
9th	42				42
10th	8				8
11th	7				7
12th	3				3
Total	60				60

Demographics

	White	59.7%
	Hispanic / Latino	13.6%
	Asian or Asian / Pacific Islander	10.4%
	Black or African American	11%
	American Indian or Alaska Native	2%
	Other or Undeclared	3.3%
	Minority Enrollment	40.3%

Gender	Male	137
	Female	17
Student to Teacher Ratio		30:1

**Demographic Data represents the most recent data obtained for 2022 – 2023 school year*

Operations

Personnel

Teacher	Education Level	Certifications	Years of Experience		Courses Taught	Dual Enrollment Qualified
			Teaching	Industry		
Janet Hartkopf	MS Curriculum & Instruction - Technology	CTE Certified	11 Years	17 Years	Security Fundamentals Ethics in IT	Y
Sam Alexander	BS Biology AS Cisco Networking	CTE Certified MTA Java	25 years	N/A	Hardware and Software Configurations LAN & Security Fundamentals	Y
Jyoti Tamboli	MS Computer Applications	CTE Certified STEM Certified	3 Years	12 Years	CYB 120 - Introduction to Computer Systems CSC 305 – Java – Computer Science A CSC 125 – AP Computer Science Principles CYB 300 – Linux Administration (RHEL)	Y

Equipment

Equipment Type	Make	Model	Quantity	Cost
Computer Kit	Basha HS Equipment List		31	\$25,000
Misc. Tools	Basha HS Lab Tool List		N/A	\$2,346.97
Locking Storage	ULINE	H-6839	1	\$1,300
Networking	Cisco	CCNA 200-301	4	\$3,638.84
PCs & Monitors	"Chromebook" type laptop with ability to use PacketTracer			

Network

- Chandler Unified School District provided network access.
- Isolated network provided for cybersecurity classrooms and lab spaces.
 - Requires separate hardware and non-district issued machines.
 - Allows access websites, resources, and facilitates meeting the learning objectives of courses.

Facilities

- School has dedicated classroom space for cybersecurity program.

- Three general purpose classrooms and one Career and Technical Education (CTE) Lab.
 - CTE lab space provides larger footprint. Consists of teaching space and space for hands on activities and equipment storage.
 - Classrooms have webcams and in-classroom microphones (2) to support video-conferencing capabilities.

Formal Learning Activities

Course	Company	Cost
CYB 240A / CNT 140 – Intro to LAN & Security Fundamentals	Cisco	* Free Courseware
CYB 240B / CNT 150 – Intro to LAN & Security Fundamentals	Cisco	* Free Courseware
CYB 300A / CIS 126DL – Linux OS	Cisco	\$30 per student lab fee
CYB 300B / CIS 238DL – Advanced Linux	Cisco	\$30 per student lab fee
CYB 400A / CIS 110 – Information Security Fundamentals	TestOut	\$2,900 per year (50 user license)
CYB 400B / CIS 111 – Ethics in Information Technology	Cengage	\$4,620 for Print Student Edition + 6 years access to online platform MindTap x 40 (price includes shipping and processing)
CYB 130 / CIS 156 – Python	Cisco	* Free Courseware

* Must be member of Western Academy Support & Training Center – WATSC (~\$500 per year)

- Reverse engineered from Chandler Gilbert Community College (CGCC) four year plan to ensure articulation and pathway for students.
- Aligns with Arizona Department of Education (DoE) CTE Network Security Technical Standards 11.1999.00.
- Completing fourth year of the program in School Year 2022 – 2023.
- Program used RedHat Linux content through 2022 – 2023 School Year. Will switch to Cisco content after 2022 – 2023 school year.

Course	Description	Syllabus	Dual Enrollment	Pre-Existing
CYB 120 / CIS 105 – Introduction to Computer Systems	Overview of computer technology, concepts, terminology, and the role of computers in business and society. Discussion of social and ethical issues related to computers. Use of word processing, spreadsheet, database, and presentation software. Includes uses of application software and the Internet for efficient and effective problem solving. Exploration of relevant emerging technologies.	Y	Y	N
CYB 230 A / BPC 170 – Hardware and Software Config & Support	This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.	Y	Y	N

<p>CYB 230 B / BPC 270 – Hardware and Software Config & Support</p>	<p>This course provides an excellent introduction to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Students participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.</p>	<p>Y</p>	<p>Y</p>	<p>N</p>
<p>CYB 240 A / CNT 140 – Intro to LAN & Security Fundamentals</p>	<p>This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.</p>	<p>Y</p>	<p>Y</p>	<p>N</p>
<p>CYB 240 B / CNT 150 – Intro to LAN & Security Fundamentals</p>	<p>This course teaches the fundamentals of networking. It covers how devices communicate on a network, network addressing and network services, how to build a home network and configure basic security, the basics of configuring Cisco devices, and testing and troubleshooting network problems.</p>	<p>Y</p>	<p>Y</p>	<p>N</p>
<p>CYB 300 A / CIS 126DL – Linux OS</p>	<p>Introduction to the Linux Operating system. Develop knowledge and skills required to install, configure, and troubleshoot a Linux-based workstation including basic network functions. Learn basic command line and Graphical User Interface (GUI) desktop environment utilities and applications. Fundamental abilities to achieve the entry-level industry certification covered.</p>	<p>Y</p>	<p>Y</p>	<p>N</p>
<p>CYB 300 B / CIS 238DL – Advanced Linux</p>	<p>Managing Linux Operating Systems including sophisticated manipulation of file structures, backup systems, printing processes, troubleshooting, user account management, hard disk maintenance and configuration, process monitoring and prioritizing, kernel customization, and system resource control. Preparation for industry certifications such as the CompTIA Linux+, the Red Hat Certified System Administrator (RHCSA), the Red Hat Certified Engineer (RHCE) and the Linux Professional Institute (LPIC-1).</p>	<p>Y</p>	<p>Y</p>	<p>N</p>
<p>CYB 400A / CIS 110 - Information Security Fundamentals</p>	<p>Fundamental concepts of information technology security. Topics include authentication methods, access control, cryptography, Public Key Infrastructure (PKI), network attack and defense methods, hardening of operating systems and network devices, securing remote access and wireless technologies, and securing infrastructures and</p>	<p>Y</p>	<p>Y</p>	<p>N</p>

	topologies. Emphasis on hands-on labs in both the Windows and Linux environments. Builds on thorough understanding of TCP/IP and security concepts and Microsoft (MS) Windows and Linux Administration.			
CYB 400B / CIS 111 – Ethics in Information Technology	Ethical issues that arise as a result of increasing use of computers, and the responsibilities of those who work with computers, either as computer science professionals or end users. Critical inquiry and review of ethical challenges in information technology business, including professional and corporate responsibility, government regulation, fiduciary responsibilities of information, infringement of intellectual property, security risk assessment, Internet crime, identity theft, employee surveillance, privacy, compliance, social networking, and the ethics of IT corporations.	Y	Y	N
CYB 130 / CIS 156 - Python	Introduction to Python programming. Includes general concepts, program design, development, data types, operators, expressions, flow control, functions, classes, input, and output operations, debugging, structured programming, and object-oriented programming.	Y	Y	N

Non-Formal Learning Activities

Camps	<ul style="list-style-type: none"> • AZ Cyber Initiative • CyberPatriot
Certifications	<ul style="list-style-type: none"> • A+ • ITF+ • Linux+ • Security Pro • Security+ • Python PCEP
Internships	<ul style="list-style-type: none"> • Open Source Integrators
Externships	<ul style="list-style-type: none"> • ElevateEdAZ • Cybersecurity and Technology Externship

Informal Learning Activities

Clubs	<ul style="list-style-type: none"> • Future Business Leaders of America (FBLA)
Competitions	<ul style="list-style-type: none"> • National Cyber League • CyberPatriot
Self-Study / Ad-Hoc Learning	Students are provided a variety of resources for additional learning outside of the classroom. Examples include cyber.org range access, Professor Messer videos, YouTube videos, and other resources.
Conferences	<ul style="list-style-type: none"> • CactusCon • WiCYS • K12 NICE Conference – Student Signing Day • Embry Riddle Aeronautical Engineering Cyber Day
Industry Events	<ul style="list-style-type: none"> • PhoenixNap Tour

Pathways

Post-Secondary	• Chandler Gilbert Community College (CGCC) Cybersecurity AAS
Trade or Certification Program	• Advanced Business Learning (ABL)
Military	• Air Force JROTC
Workforce	• Kelly Technologies

Equipment, Hardware, and Software Requirements

Intro to Computer Systems

- MS Office Apps
- Internet access
- eBook curriculum

Hardware / Software Lab Setup

- Lab Tables w/integrated power
- Anti-Static Mat on the tables
- eBook curriculum
- Packet Tracer software

Computer Kit – the kit requirements will vary upon how you choose to allow students to connect for the purpose of downloading OS and various drivers (PacketTracer is now on the approved software list)

Component	Quantity
1. Motherboard – ATX (full size)	31
a. LGA1200 – Intel	
2. CPU w/heat sink & fan	31
3. Graphics Processing Card	31
4. RAM (8GB) - recommended by Cisco (2 X 4GB suggested) needed for VM practice in curriculum	31
5. Case (ATX)	31
6. Ethernet Card	31
7. PCI / PCIe	31
<p><i>This storage setup will allow students to configure their machine and NOT have to reverse all their work for the next class. Each student would be assigned an SSD that would remain in the classroom and used for their work in the lab</i></p>	
8. Storage	31 Bays 1/Tray per SSD 1 /per student
a. Swappable SSD	
i. Bay (30) - ~\$25/ea (CDW)	
ii. Trays (1 for each student) - ~\$11/ea (CDW)	
b. SSD – 120GB (1 for each student) - ~\$30/ea (CDW)	

Cables

- Ethernet UTP bulk cable (CAT5e)
- Stranded UTP bulk cable (CAT5e)
- RJ45 connectors – Stranded and Solid Core
- RJ45 Network Cable Tester
- Crimpers
- Multimeter
- Networking scissors
- Cable stripper
- PC Power Supply Tester
- Anti-Static Duster
- Network Cable Tester

Tools

- 11-piece PC computer tool kit
- Anti-static wrist strap

Printer

Switch / Router

HDMI Monitors



Stainless Steel Security Cart - 36 x 24 x 69"






Price Each		Order in multiples of: 1
Model#	1	3 +
H-6839	\$1,370.00	\$1,320.00







1



Maximum Quantity 2.

[ULINE Search Results: Stainless Steel Mobile Security Cage](#)

Basha High School Lab Tool Inventory

Item	Qty	Vendor	Picture	Total
Digital Multimeter, MSR-C600	2	Amazon	 <p>Etekcity Digital Clamp Meter Multimeter AC Current and AC/DC Voltage Tester with Amp, Volt, Ohm, Continuity,...</p> <p>★★★★★ ~ 6,202</p> <p>Limited time deal</p> <p>\$24⁹⁹ \$29.99</p> <p>prime Get it as soon as</p>	\$49.98
PC Power Supply Tester	2	Amazon	 <p>20/24 4/6/8 Pin Computer PC Power Supply Tester with LCD Display SATA, HDD</p> <p>★★★★★ ~ 97</p> <p>\$18¹⁹</p> <p>prime</p> <p>FREE delivery Wed, Apr 19 on \$25 of items</p>	\$36.38
11 Piece PC Computer Tool Kit	31	Amazon	 <p>StarTech.com 11 Piece Computer Tool Kit with Zippered Vinyl Carrying Case (CT</p> <p>★★★★★ ~ 1,172</p> <p>\$26⁶⁸ \$29.99</p> <p>Get it Mon, Feb 28 - Thu, Mar 3</p> <p>FREE Shipping</p> <p>Only 6 left in stock - order soon.</p> <p>More Buying Choices</p> <p>\$26.42 (16 new offers)</p>	\$827.08
Anti-Static Wrist Strap	5	Amazon	 <p>ESD Anti-Static Wrist Strap Components, DaKu</p> <p>Anti-Static Wrist Straps Equipped with Groundi</p> <p>★★★★★ ~ 262</p> <p>\$11⁹⁹ (\$2.00/Item)</p> <p>FREE Shipping on orders over \$25 shipped by Amazon</p>	\$59.95
MetroVac Anti-Static Electric Duster	2	Amazon	 <p>MetroVac ED-500-ESD Anti-S</p> <p>Pack</p> <p>★★★★★ ~ 79</p> <p>\$129⁹⁹</p> <p>prime Get it as soon as Tomorrow, Feb 24</p> <p>FREE Shipping by Amazon</p> <p>More Buying Choices</p> <p>\$78.77 (5 used & new offers)</p>	\$259.98

<p>Cable Crimpers RJ45 Crimp</p>	<p>30</p>	<p>Amazon</p>	 <p>Cable Matters Modular RJ45 Crimp Tool (Ethernet Crimper) with Built-in Wire Cutter and Stripper - 10-Pack Cat6 RJ45 Connectors Included ★★★★☆ ~ 144 \$13.99</p>	<p>\$419.70</p>
<p>RJ45 Connectors SHD CAT6 Solid/Stranded Core</p>	<p>10</p>	<p>Amazon</p>	 <p>Sponsored Cable Matters 100-Pack CAT6 RJ45 Modular Plugs (RJ45 RJ45 Plugs) for Solid or Stranded UTP Cable ★★★★☆ ~ 654 \$14.49 \$18.99 prime Get it as soon as Tomorrow, Feb 24 FREE Shipping on orders over \$25 shipped by Amazon</p>	<p>\$144.90</p>
<p>NavePoint CAT5e, Solid Bulk Ethernet Cable UTP</p>	<p>1</p>	<p>Amazon</p>	 <p>NavePoint CAT5e (CCA), 500ft Cable, 24AWG 4 Pair, Unshielded ★★★★☆ ~ 73 \$56.42 prime Get it as soon as Sun, Feb 25 FREE Shipping by Amazon Only 11 left in stock - order soon.</p>	<p>\$56.42</p>
<p>Belkin 250 ft CAT5e Stranded UTP Bulk Networking Cable</p>	<p>1</p>	<p>Amazon</p>	 <p>Belkin 250-Foot Cat5e PVC Stranded UTP Bulk Networking Cable (Gray) Visit the Belkin Store ★★★★☆ ~ 86 ratings 16 answered questions Price: \$63.03 & FREE Returns Get \$60 off instantly: Pay \$3.03 \$63.03 upon approval for the Amazon Prime Store Card. No annual fee. Available at a lower price from other sellers that may not offer free Prime shipping. Size: 250-Foot 250-Foot 1000 feet 1000 feet Color: Gray</p>	<p>\$63.03</p>
<p>RJ45 Network Cable Tester for LAN Phone/RJ45 WireTestTool</p>	<p>30</p>	<p>Amazon</p>	 <p>iMBAPrice - RJ45 Network Cable Tester RJ45/RJ11/RJ12/CAT5/CAT6/CAT7 UTP ★★★★☆ ~ 2,934 \$9.99 prime Get it as soon as Tomorrow, Feb 24 FREE Shipping on orders over \$25 shipped by Amazon More Buying Choices \$7.90 (10 used & new offers)</p>	<p>\$299.70</p>
<p>Networking Scissors</p>	<p>5</p>	<p>Amazon</p>	 <p>Klein Tools 21010-6-SEN Free-Fall Snip, Scraper, File, Serrated Blades ★★★★☆ ~ 998 \$19.97 prime Get it as soon as Fri, Feb 25 FREE Shipping on orders over \$25 shipped by Amazon More Buying Choices \$17.57 (11 used & new offers)</p>	<p>\$99.85</p>

Network Cable Tester	1	Amazon		Ubrand Network Cable Tester, RJ45 RJ11 Multi-Fur Cable Collation, Network & Telephone Line Test, R ★★★★★ ~ 175 \$20 ⁹⁹ - \$21 ⁹⁹ FREE delivery Also available in Yellow	\$22
Mini Wire Stripper	1	Amazon	 <p>Mini Wire Stripper, 6 Pcs Network Wire Stripper Punch Down Cutter for Network Wire Cable, RJ45/Cat5/CAT- 6 Data Cable, Telephone Cable and...</p> ★★★★★ ~ 591 \$7 ⁹⁹		\$8
Total Cost					\$2,346.97

Cisco CCN 200-301 Standard Kit



Cisco CCNA 200-301 Standard Kit

\$749.98

SKU:
SKU-3020

Access Server: Optional

Choose Options

Rack Options: Optional

Mini 12U Deluxe Rack & Rack Kits (+ \$13)

Optional Serial Cards and Cables Bundle: Optional

Smart Serial Bundle (+ \$150.00)

Supplemental CCNA Training DVD: Optional

(+ \$20.00)

Optional Wireless Access Point: Optional

(+ \$60.00)

FTDI Console Cable Upgrade: Optional



Hardware Included:

- Three Cisco 1841 256/64 Routers (Dual FE router supports 15.1(4) Advanced IP Services)
- Three Cisco 2960-TT-L Switches (Supports 15.0(2) IOS) and IPv6 addressing and can do very limited Layer 3 static routing.
- Three Ethernet Patch Cables
- Three Ethernet Crossover Cables
- Cisco Console Kit
- Power Cords

Additional Items Included:

- 450 Page CCNA 200-301 Lab eWorkbook Covering 60+ Labs Plus Bonus Labs That Go Beyond the Scope of CCNA For Extra Real World Experience! **(\$57.99 value)**
- 864 Page Bootcamp & Theory eBook that covers every 200-301 CCNA Topic Plus More! **(\$49.99 value)**
- How & Why We Subnet eWorkbook **(\$24.99 value)**
- Two Practice Exams. Both with 101 Questions, Answers and Explanations **(\$15.98 value)**
- CCNA CRAM Sheet **(\$14.99 value)**
- TCP/IP Study Poster **(\$9.99 value)**
- CertificationKits TFTP Server
- CertificationKits Subnet Calculator
- CertificationKits Binary Bits Game
- 50 CCNA Instructional Videos
- Cisco Network Assistant
- Cisco Router Password Decryptor
- Cisco VPN Client 5.0.04.0410
- Port Scanner nmap-7.80
- npcap-0.9987 & WinPcap 4.1.3
- WireShark 1.10.05 & 3.2.1
- TeraTerm & Putty Terminal Emulators
- VirtualBox 6.1.4
- IOS Backup as noted above for the routers and switches
- Cisco Configuration Professional (CCP) 2.8 for 1841/2800 Series Routers

NAME OF VENDOR Certification Kits - Cisco

ADDRESS 1212 S Naper Blvd Ste 119-329

CITY Naperville **STATE** IL **ZIP CODE** 60540

PHONE NO. (866) 950-2478 **FAX NO.**

***W9 FORM NEEDED FOR NEW VENDORS**
***MUST INCLUDE MINUTES FOR STUDENT ACTIVITY MONEY**

QUANTITY	CAT NO.	DESCRIPTION	UNIT PRICE	TOTAL AMOUNT
4		CCNA Standard 200-301 Kit	459.99	1,839.96
4		Mini 12U Deluxe Rack & Rack Kits	139.99	559.96
4		Smart Serial Bundle	150.00	600.00
				0.00
				0.00
				0.00
				0.00

Print Name of Authorized Signer: [Redacted]

Minutes Provided: No

SUBTOTAL	2,999.92
TAX	
SHIPPING	
TOTAL	2,999.92

<https://shop.certificationkits.com/cisco-ccna-200-301-standard-kit/>



certification Kits
CertificationKits Invoice for Order #36468

CertificationKits
1212 S Naper Blvd Ste 119-329
Naperville
60540
IL

Billing Details	Shipping Details
------------------------	-------------------------

Order:	#36468	Order Date:	Jan 19th 2021
Payment Method:	Check/ Wire/ Phone (\$3,638.84)	Shipping Method:	UPS

Order Items

Qty	Code/SKU	Product Name	Price	Total
4	SKU-3020	Cisco CCNA 200-301 Standard Kit	\$779.97 USD	\$3,119.88 USD
		Rack Options: Mini 12U Deluxe Rack & Rack Kits (+ \$139.99)		
		Optional Serial Cards and Cables Bundle: Smart Serial Bundle(+ \$150.00)		
		Supplemental CCNA Training DVD: No		
		Optional Wireless Access Point: No		
		FTDI Console Cable Upgrade: Yes		
		One-Time Print Right for Lab Workbook: No		
		Extended Warranty: 1 Year (included)		
4	SKU-2727	9 Outlet PDU	\$34.99 USD	\$139.96 USD
			Subtotal:	\$3,259.84 USD
			Shipping:	\$379.00 USD
			Grand Total:	\$3,638.84 USD

Arizona Department of Education CTE Recommended Equipment List

Arizona Department of Education

Career and Technical Education

Recommended Equipment List

Program: NETWORK SECURITY
CIP#: 11.1999.00

NOTE: The following items and descriptions are the recommended equipment guidelines for each CTE Network Security program. Please note that this list of recommended items does not necessarily need to be supported financially by Federal Perkins or State Priority funding sources. In many cases, local school district funds are used to purchase items on a regular basis (i.e. furniture, consumables, etc.) Further, please understand that this is not an exhaustive list. Local program and business needs may necessitate the purchase of additional equipment and software resources, as may the rapidly-changing nature of the industry-specific technologies used in the program.

Please contact ADE-CTE Program Specialist Tracy Rexroat (tracy.rexroat@azed.gov) if you have questions regarding the appropriateness of any item you are considering for addition to your CTE Network Security program.

Recommended Equipment and Software	
Item	Notes
Cable Cutter, Coax	
Crimp Tool W/ Stripper, RJ11, RJ45	30
File, Flat Needle	
Flashlight, Tactical L.E.D.	5
Forceps, Straight w/Grip	
Handle, For Blades, Drive-Loc	
Hex Keys Set, Fold-Up .050" to 3/16"	2
Insertion/Extraction Tool	
Nutdriver Blade, 3/16" 1/4, 5/16, 3/8	
Pliers, Diagonal 4" W/Spring	
Pliers, Long Nose 4 3/4", 6" w cutter	
Pliers, Slip Joint 6"	
Pliers, Vise-Grip Long Nose 6"	
Punchdown Tool W/110 Blade	5
Receptacle Analyzer	
Screwdriver, Phillips #0 x 2", 1x3, 2x4	30
Screwdriver, Slot 1/4" x 6"	
Screwdriver, Slot 3/16" x 4"	
Screwdriver, Slot 3/32" x 2"	
Screwdriver, Stubby 2 in 1	
Soldering Iron, 25 Watt 3-wire	3
Telephone Line Tester	
Tone Line Aid W/Volume Control (Multimeters)	
Tone Tracer, High Powered (Circuite Testers)	
Trimpot Tool	
Wire Strippers, "T" 16-26 (1)	
Wrench, Adjustable 6" Ergonomic	
Desktops/ Laptops/ or I-pads	31
Routers	12
Servers	2
Switches	12
Software tools for Analysis	
network protocol analyzer, e.g. TShark., iPerf3 to support tuning of many parameters buffers, and protocols (TCP, UDP, SCTP with IPv4 and IPv6).	Wireshark and Packet Tracer
security scanner to create a map of the network.	
debugger program to find communication and/or data problems in SNMP monitoring configurations.	
IP address and port scanner.	
IP calculator	

Monitoring & Logging	
Network monitoring software solution to dig deep into the health and integrity of your systems and network. An approach to monitoring.	
system usage software.	
NetFlow Analyzer	
Server software	Red Hat, Ubuntu, MS Server, AWS Cloud, VMWare
Configuration & Transfer software	Clonezilla, Tera Term, puTTY, UDP Cast
a multi-vendor Python library	Internet access to IP & PMP Modules
network device software.	Firmware access for devices
Platform supports	Operating system keys for each student
TFTP Server	Can be installed on server software
SFTP/SCP Server software	Can be installed on server software
For Network troubleshooting https://www.pluralsight.com/blog/it-ops/network-troubleshooting-tools	
Free tools: https://www.networkmanagementsoftware.com/top-17-free-tools-for-network-administrators/	
Sensors- pressure, magnetic, resistive, capacitance, photo electric	
PLCs	
Motors	
Actuators	
relays	
IC controllers	
Breadboard	
switches	
Printed circuit boards PCBs	
Power supplies	
Programmable manipulators	
1 cartesian	
(2) gantry	
(3) cylindrical	
(4) spherical	
(5) articulated	
(6) SCARA	
Robot controls	
1 Point to point (PTP)	
2 Continuous Path control	
3 Controlled path control	
Automation and programming control tools	
Programable Computer Numeric control	
Direct Numeric Control DNC	
Printed Circuit Boards (PCB's)	
computer-integrated manufacturing (CIM)	
HMI software	
PAC, PLC and controllers software	
*Must meet the guidelines for specialized computing equipment as outlined on the "CTE Equipment Guidelines" at www.azed.gov/cte/grants	

Additional Items:

Network Scissors:	10	Motherboard:	31
CAT6 Cable:	500ft	Removable HD Bay:	31
RF45 Connectors:	1000	SSD:	31
Network Patch Panel:	4	HDD:	31
Anti-Static Electric Duster:	2	Power Supply Units:	31
Anti-Static Wrist Strap:	30	CPU:	31
PC Computer Tool Kit:	30	Graphics Card:	31
Digital Multimeter:	2	Tower:	31
Computer Kit:	31	Color Printer:	1
RAM:	31		

Appendix B: Questionnaire and Interview Guide

Interviewee Questionnaire

1. What is your current role or job title?
2. If applicable, what academic degrees do you hold?
3. If applicable, what industry certifications do you hold?
4. How many years of experience do you have in secondary education?
5. What courses have you taught at the secondary education level and how many years have you taught each course?
6. If applicable, how many years of experience do you have in industry work related to cybersecurity, information technology, computer science, or related field?
7. What was your role in developing the cybersecurity education program at your institution?
8. If there is anyone else that you believe had input into the program and can provide insight into program development and operations, please provide them with my contact information and have them contact me.

Program Profile Questionnaire Questions

1. Describe the operational elements of the cybersecurity education program.
 - a. Instructors (Education, Certifications, Years of Experience (Teaching / Industry), Courses Taught, Dual Enrollment Qualified (If so, What Courses)).

Teacher	Education Level	Certifications	Years of Experience		Courses Taught	Dual Enrollment Qualified
			Teaching	Industry		

- b. Equipment (Type, Make, Model, Number, Cost)

Equipment Type	Make	Model	Quantity	Cost

2. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.
 - a. What courses are included in the cybersecurity program?
 - b. What are the course descriptions for courses within the cybersecurity program?
 - c. Can you provide the syllabi for the courses within the cybersecurity program?
 - d. Is the course dual enrollment?
 - e. Did the course exist before the development of the cybersecurity program?

Course	Description	Syllabus	Dual Enrollment	Pre-Existing

Interview Questions

1. What was the motivation for starting a cybersecurity education program at your institution?
2. Describe how the cybersecurity education program was developed at your institution.
 - a. What standards, guidelines, or frameworks were used to develop the program?
 - b. How were the courses selected for inclusion in the cybersecurity program at your institution?
3. Describe the operational elements of the cybersecurity education program.
 - a. Instructors
 - i. How are qualified teachers identified or hired to teach cybersecurity courses?
 - ii. If applicable, describe the challenges in finding qualified instructors for cybersecurity courses.
 - b. Equipment
 - i. How was the equipment listed identified or determined to be needed to support the selected courses?
 - ii. If applicable, describe the challenges in procuring the equipment necessary to support the selected courses.
 - c. Networks
 - i. Describe the networks that students use for their cybersecurity curriculum and assignments.
 - ii. If applicable, describe the challenges in operating on those networks.
 - d. Facilities
 - i. What facilities are used by students in the cybersecurity program?
 - ii. Are these facilities utilized by students outside the cybersecurity program and if so by what programs?
 - iii. Describe the process for acquiring these facilities.
 - iv. If applicable, describe the challenges in obtaining these facilities to support the selected courses.
4. Describe the formal learning activities. Formal learning is the type of learning that is intentional, organized, and structured. Formal learning opportunities are usually arranged by institutions. Often this type of learning is guided by a curriculum or other type of formal program.
 - a. Why were these courses selected for inclusion in the program?
5. Describe the non-formal learning activities. Non-formal learning is a type of learning that may or may not be intentional or arranged by an institution, but is usually organized in some way, even if it loosely organized. There is no form of credits granted in non-formal learning situations. Examples of non-formal learning activities include camps, certifications, internships, and apprenticeships.
 - a. Based on the provided definition and examples, what non-formal learning activities are incorporated in the cybersecurity program?
 - b. How do these activities support the cybersecurity program and cybersecurity students?
6. Describe the informal learning activities. Informal learning is a type of learning that is never organized. Rather than being guided by a rigid curriculum, it is often thought of as experiential and spontaneous. Examples of informal learning activities include clubs, competitions, self-study / ad-hoc learning, conferences, and industry events.

- a. Based on the provided definition and examples, what non-formal learning activities are incorporated in the cybersecurity program?
 - b. How do these activities support the cybersecurity program and cybersecurity students?
7. Describe the pathways for students. Students have four primary options after graduating from secondary education: go directly into the workforce, join the military, enter a trade or certification program, or attend post-secondary education.
 - a. How does the cybersecurity program prepare students for the various pathways outlined above?
 - b. How does the program track students upon graduation from the cybersecurity program?

Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation

Ryan Straight
ryanstraight@arizona.edu
Department of Cyber, Intel, & Information Operations
University of Arizona
Tucson, AZ 85721

Abstract

As the cyber domain grows into each aspect of our lives, so does the need to expand approaches in understanding and researching cybersecurity and cybersecurity education. By focusing on a novel methodology within these fields—postphenomenology—this paper seeks to demonstrate its cyber-related usefulness and application. At its core, postphenomenology is the study of technological mediation and the myriad ways of uncovering and understanding it and its consequences. In tracing a line from classic phenomenology to the exploration of cyborg technological intentionality, I suggest an applied postphenomenology that addresses calls for holistic and multidisciplinary cybersecurity education. By incorporating postphenomenological methods into cybersecurity pedagogical research and practice, educators and students alike can come to deeper and more meaningful realizations and applications stemming from human-technology-world relations.

Keywords: postphenomenology, methodology, mediation theory, intentionality, phenomenology, multidisciplinary

Recommended Citation: Straight, R., (2024). Doing Postphenomenology in Cybersecurity Education: A Methodological Invitation. *Cybersecurity Pedagogy and Practice Journal*, 3(1), pp.64. <https://doi.org/10.62273/TWSH7587>

1. INTRODUCTION

As cybersecurity and cybersecurity education are still relatively nascent fields, a multidisciplinary and varied approach is appropriate to understanding and identifying opportunities to fill gaps and respond to needs unknown. This paper seeks to provide one such approach, bringing the lens of postphenomenology to bear on the process. Through “classical” phenomenology, Ihde’s postphenomenology, and Rosenberger’s and Verbeek’s expansions thereof, and the work of others, I argue for the application of Adams and Turville’s “postphenomenology of practice” to cybersecurity education. To achieve this, I provide a brief introduction to phenomenology and its connection to technology before delving into postphenomenology, an empirical philosophy of technology that explores the relation between humans, technology, and the world. I will then present postphenomenology’s potential impact on the cybersecurity domain and apply postphenomenology to cybersecurity education, specifically. Suggestions for postphenomenological approaches to cybersecurity pedagogy and potential topics for analysis follow. First, however, I will explore the foundational cybersecurity education landscape.

2. NEEDS IN CYBERSECURITY AND CYBERSECURITY EDUCATION

Cybersecurity is, unsurprisingly, entirely reliant on *people* and *technology*. Without either, there is no cyber domain. However ubiquitous technology may be within the field, access to education is often strikingly lacking in breadth and depth. Described as “infrequent and uneven,” over half of public schools in the United States provide no cybersecurity education, with most educators identifying areas like cyber law, cryptography, and artificial intelligence as entirely absent (Chiosea, 2020).

Projections estimated a global shortfall of 1.8 million cybersecurity positions by 2022 (Pinchot et al., 2020). Instead, the global workforce gap reached upwards of 3.4 million even while adding nearly a half million jobs in the previous year ((ISC)², 2022). Consequently, tremendous effort has been placed on workforce pipelines and cybersecurity education to address the workforce gap and to develop a more cybersecure population. Wagner (2023) examines cybersecurity education frameworks, platforms, and workforce pathways, emphasizing an established need for all-level, all-domain approaches. Useful among these is the *K-12*

Cybersecurity Learning Standards (Cyber Innovation Center & CYBER.ORG, 2021), which focuses on computing systems, digital citizenship, and security. These themes or concepts are further broken down into sub-concepts, topics, and “gradebands” for age-appropriate examples and clarification. We will return to the implementation of these standards shortly.

While much cybersecurity education research demonstrably focuses on business and workforce development, humanistic or philosophical approaches are generally relegated to the realm of ethics. Ethics—specifically cyberbullying—is a frequently addressed topic in K-12 cybersecurity education (Chiosea, 2020). Beyond ethics at one end and purely technical areas like network communications on the other, a vast range of fields and topics are worthy and need investigation and analysis. In the following pages, one approach—an applied postphenomenology—is presented as a robust addition to the methodological toolbox allowing delving deep into the lived experiences associated with technology and the cyber domain, as well as varied pedagogical approaches.

3. PHENOMENOLOGY AND TECHNOLOGY

Prior to exploring *postphenomenology*, we must explore phenomenology itself. Phenomenology is generally known as the philosophical approach to understanding *being in the world* and the experiences therein. It is a wholly qualitative approach, attempting to expose a pure, unvarnished, raw experience and learn from it. In this way, “doing” phenomenology (and postphenomenology, as we will see) is a unique approach to revealing how one is situated within the lifeworld.

Phenomenology can be thought of as “a radical, anti-traditionalist style of philosophizing [seeking] to avoid all misconstructions and impositions placed on experience in advance” (Moran, 2000, p. 4). It is a method of identifying themes across diverse experiences and of making known the connections between what *is* and how it is *perceived to be*. As such, one’s intention plays a key role, with the overarching goal being “to discover and describe consciousness by means of studying the essential conscious elements, acts, structures, and their interrelation” (Gutland, 2018, p. 10).

While a full and comprehensive introduction to phenomenology is outside the scope of this paper, a brief venture into a classic example with

technology is warranted: generally, technology is seen as something to overcome. Phenomenology points to the difference between technology working as intended and technology hindering one's actions. The carpenter's hammer is *Zhuhanden*, or *ready-to-hand*, representing the tool as a functional extension of the self (Heidegger, 1927). A carpenter using a working hammer does not direct her intention to the hammer; rather, she directs it to the *nail*. Conversely, a technology that *does* become a hindrance (*Vorhanden*, or *present-at-hand*) no longer expands one's abilities and self but rather is *dealt with*, a situation to overcome (Blitz, 2014). Even if that hammer is ready-to-hand (usable to hammer a nail), it holds the potential to become present-at-hand (a paperweight) at any time.

Postphenomenology turns this on its head, positing that rather than *hindering* experiential understanding, technology instead *mediates* it, worthy of empirical analysis. This is the first step toward the cybersecurity and cybersecurity education connection, which requires deeper exploration.

4. POSTPHENOMENOLOGY

Postphenomenology is presented as the anti-essentialist, empirical, pragmatic methodological successor of phenomenology (Ihde, 1990) and can be defined as a "phenomenology that attends to specific technologies and the existential and epistemological differences they may be making to the lifeworld" (Adams & Turville, 2018, p. 4). It reconsiders technology not as a barrier or hindrance but an invitation through reifying phenomenology's focus on intentionality.

Ihde (1990) initiated the field, describing four core relations between humans, technology, and the world. These describe how amalgams of human-and-technology and technology-and-world are understood, and the direction and path of intention. These are provided alongside typograms for illustration below, along with examples in cybersecurity education to assist in drawing practical connections between the methodology and the domain.

The *embodiment* relation is one in which the human and technology function as one with intention directed at the world:

(Human - Technology) → World

Or, in the case of the carpenter,

(Carpenter – Hammer) → Nail

The carpenter-hammer unit directs intention at the nail. In a cybersecurity context, this is easily understood as user-keyboard directing intention to a website or application. Likewise, it could be explored as user-software directed at a network. The I/technology/world antecedents are malleable, as we will see shortly.

The second relation is the *hermeneutic*, a translatory and interpretational relation, such as reading the time from a clock or examining an x-ray. The user directs their intention toward the technology that, itself, represents something about the world.

Human → (Technology - World)

The interpretive nature of this relation is ostensibly based on trust—one trusts the clock to not be fast or slow—but can lead to unexpected or undesirable outcomes, such as instrumental error resulting in ill-advised decisions (a radar altimeter in a helicopter providing an incorrect distance to the ground, for example). In the cyber domain, one can easily apply this to interpreting network traffic to understand atypical behavior or interpreting email content to identify phishing.

Alterity is the treating of technology as "other." Mundane as a blender or advanced as anthropomorphized digital assistants, it is engaging technology as a separate entity. Like Alexa, where the alteric nature of the interaction is clear (as one would speak to another), the same core relation describes the use of a battery, a safety harness, or lawnmower. With the growing popularity and use of large language models (LLMs) like ChatGPT (OpenAI, 2023), understanding this relation becomes crucially important.

Human → Technology – (– World)

In a cyber context, for example, this could be simply interacting with tools like USB drives or IoT devices.

Finally, the *background* relation deals with technology that, while having a direct impact, is part of the environment. An air conditioner, for example, or smart lights. It is typically the breakdown-becoming *present-at-hand*-of these technologies that bring awareness of their existence and use to the foreground. They are represented as:

Human – (Technology / World)

For the average user, most engagement in the cyber domain appears relegated to the background: security breaches, on-path attacks, unencrypted data transfer, and so on.

Technic relations are not mutually exclusive; rather, they frequently overlap. When driving a vehicle, one embodies the machine as they *feel* the road beneath them through the controls, interprets the speed via the speedometer, works the steering wheel and pedals as alteric tools.

As technologies grow more advanced and permeating more aspects of our lives and bodies, other relations are needed. Peter-Paul Verbeek (2008a; 2015) has expanded these relations through continuing research on technological mediation theory and the concepts of *hybrid* and *composite* intentionalities. These in turn lead to new technic relations beyond Ihde’s original four (see Table 1 below):

Cyborg / Fusion	(Human / Technology) → World
Composite	Human → (Technology → World)
Immersion	Human ← → Technology / World
Augmentation	(Human – Technology) → World → (Technology – World)

Table 1: Hybrid and Composite Intentionalities

The “cyborg” or “fusion” relation is typified by a pacemaker: human and machine combine in such a way that one does not function meaningfully without the other. The “composite” relation progresses the hermeneutic relation in that “humans are directed here at the ways in which a technology is directed at the world” (Verbeek, 2008a, p. 393), like a thermal camera displaying what *it* sees that we cannot. An “immersion” relation is akin to the background relation with the difference being the intention is bi-directional (a “smart mirror,” for example, fusing technology with the world around it, while reactions become mutual). The “augmented” relation describes a feedback loop: through augmented reality glasses, for example, the user and the glasses are directed toward the world, at which point the glasses “react” to the world, feed that information back to the user, and the user then reacts to *that*.

Identified in these four newer relations, the distance between technologies and the self,

approaches zero (i.e., background → immersion, or embodiment → cyborg) and the need to understand new mediation grows in tandem. As stated at the outset, since *all* cybersecurity and cybersecurity education revolve around interactions between humans and/though technology, the need for a deep, meaningful understanding cannot be overstated. And, while “cyborg cybersecurity” may seem relegated to edge cases in medicine or even science fiction, our submergence in the digital realm points toward a growing and inescapable importance. By applying postphenomenological methodology, access to and understanding of this may grow in unexpected ways.

5. APPLIED POSTPHENOMENOLOGY

A variety of postphenomenological accounts of wide-ranging technologies and mediated experiences have been performed in recent years, such as a parent encountering a child through an ultrasound scan (Verbeek, 2008b), an exploration of the world through cochlear implants (Besmer, 2012), even an examination of park benches (Rosenberger, 2020). Lacking dogma, the method for approaching these studies vary as much as their topics. That said, as we mean to apply postphenomenology to cyber and cyber education, three concepts need described: multistability, transparency, and variational analysis. Combined, these make up a large portion of the postphenomenologist’s toolbox.

Technologies have multiple uses. Some uses are easily identified and implemented (an *affordance*, the ways technologies invite a particular use; a doorknob *affords* turning). In postphenomenological terms, this is *sedimentation* (Rosenberger, 2009). A basketball affords a variety of uses but bouncing is *highly sedimented* and is its *dominant stability*. However, a postphenomenological analysis strives to find the *multistability* of a particular technology. How could it be used otherwise? What could it mean? How does it allow new experiences, intended or otherwise? The multistability of technologies is at the core of postphenomenology (see Ihde, 2012).

Transparency (Ihde, 1990), then, can be understood as the degree to which a technology recedes into the background during use. The conscious manipulation or awareness fades and one’s intention flows effortlessly to its ultimate target. Driving a car or touch-typing on a keyboard, for example. This is closely related to “field composition” or “field of awareness” (Rosenberger & Verbeek, 2015, p. 23), in which

one's perception shrinks, narrows, or perhaps simply focuses, such as no longer noticing what happens beyond the edges of the screen when viewing a film.

The method of exploring and answering these questions is the most fundamental of postphenomenological methods: variational analysis (literally, analyzing the variations in the ways a technology is used and mediates experience). This is precisely the process that exposes multistability through imagining, experimenting, or investigating the uses of technologies. Rosenberger (2020) describes a next-step: variational cross-examination, allowing us to "learn things *about particular stabilities* through their comparison *with one another*" (p. 6; emphasis in original). He elaborates:

...it can be especially difficult to investigate a dominant stability (whether through postphenomenology or any other perspective). It calls for an effort to see through normalcy, to extract things from their contexts (at least provisionally), to look past many specific design elements, and to break potentially deeply-ingrained habits of perception and understanding. The postphenomenological method of variational cross-examination can be useful for this kind of project. (p. 6)

Still, though we have examples of cases and methodological steps to take, how precisely does one *do* postphenomenology? How to implement this approach needs to be unpacked before doing the application. Adams & Turville (2018) provide something of a roadmap for practicing this philosophy of technology in education, stemming from van Manen's *Phenomenology of Practice* (see Van Manen (2014)). "The ambition of phenomenology of practice is simple: to describe and reflect on a phenomenon of professional or personal interest by attending to the prereflective or everyday lifeworld" (Adams & Turville, 2018, pp. 11–12). Through these approaches, we begin to tease out the ways in which postphenomenology may shed light on a complex, multifaceted domain like cyber. Concrete steps for variational data generation—that is, how one might go about gaining access to these stabilities—are described below.

Bringing this phenomenology of practice into a *postphenomenology of practice* (or, an "applied postphenomenology") strives for "thematizing of materiality, particularly in the form of instruments and devices which we make 'worlds'

available to us which were previously unexperienced and unperceived" (Ihde (2003) in Adams & Turville (2018)). Specifically, one must generate data for a postphenomenological analysis, as with any research. Four methods of phenomenology of practice and postphenomenological data generation described by Adams and Turville are outlined below. Explicit ties to a postphenomenology of cybersecurity education are described in the section following.

1. **Prereflective: self-observational anecdotes.** A method relying on the observer to describe, with a distanced kind of clarity and lack of judgment, her own "concrete, lived-through" experiences.
2. **Prereflective: interviews.** Interviews, but specifically with a goal to "elicit lived experience descriptions (LEDs) about the research participant's everyday engagements and encounters with the technology of interest" (Adams & Turville, 2018, p. 15).
3. **Prereflective: observational anecdotes.** Observing the experiences of others is yet another method. This method may lack a certain depth provided by others but may equally lead to accessing experiences and uses of technologies of which users themselves may be unaware.
4. **Reflective: the breakdowns.** Reflecting on technological breakdowns naturally demonstrates and brings to light its multistability and stabilities, while exposing it to meaningful variational analysis. More simply: what happens when the tool breaks, and what could it tell us about the tool, ourselves, and the person-tool-world amalgam?

Key here follows Verbeek's insistence that intentionality "needs to be understood as the specific ways in which specific technologies can be directed as specific aspects of reality" (2008a, p. 6). This provides an opening to understanding how this methodology could be applied to cybersecurity and cybersecurity education. With these four approaches to applying postphenomenology to specific situations, combined with the variational analysis and cross-examination methods, we may explore practical applications. These methods may sound familiar upon reflection. Indeed, while phenomenological approaches to exploring cybersecurity—especially deception—exist (see Majkut et al. (2009)), explicit *postphenomenological* explorations of cybersecurity and cybersecurity education are missing from the literature. First, though, we will explore postphenomenological applications

outside the cyber domain to assist in making the jump.

6. PRACTICAL APPLICATIONS

Postphenomenological explorations involve considerable creative exploration and observation of people's lived experiences. Prior to attempting concrete connections to cyber and cybersecurity education, there is value to *priming the pump*, as it were, by delving into existing postphenomenological applications across domains.

Postphenomenological approaches can be seen ranging in research on fitness, especially the technological methods of tracking fitness (Ayas Önel & Akyaman, 2021; Zheng, 2021), to ethics (Morrison, 2020; Verbeek, 2023). The medical field has been especially ripe for postphenomenological analyses, whether these are the sonographic experiences parents have of the fetus in utero (Verbeek, 2008b) or analyses of assistive technology used by older people (Lynch et al., 2022).

Attempts to bring the benefits and insights provided by postphenomenological analysis to the development of other frameworks have also been made. For example, Vindenes and Wasson (2021) provide a postphenomenological framework for studying virtual reality and user experience, describing a "simulated subjectivity" that, through technologically-mediated immersive experiences, can lead to promoting empathy and revealing "otherness."

Research in education has benefitted from postphenomenological application, such as Wellner & Levin's (2023) focus on Papert's constructionist pedagogical framework, drawing insightful and explicit connections between the "four qualities" of learning environment personalization (embodiment), computational thinking (hermeneutics), microworlds (alterity), and the democratization of education (background relations). Likewise, the work of Adams & Turville, which is referenced here at length, provides actionable approaches to marrying postphenomenology and pedagogy, leading to a "posthuman inquiry" method.

The myriad fields postphenomenology can be applied to are demonstrably as numerous as the ways to apply it. Understanding these while having concrete examples of postphenomenological studies makes for a smoother integration into the cyber domain, cybersecurity education, especially.

7. POSTPHENOMENOLOGICAL CYBERSECURITY AND EDUCATION

Adams & Turville (2018), in *Doing Postphenomenology in Education*, demonstrate precisely why this particular methodology is relevant and applicable in this context: it "involves attending to the unique differences a particular technology makes to teaching practice, knowledge apprehension, and pedagogical meaning" (p. 20). When "...my email tugs at me to check it, my buzzing iPhone insists that I answer it" (Adams & Turville, 2018, p. 12), the relationship between self and technology determines the reaction. Typically, it is steeped in trust, familiarity, even muscle memory. The question arises: should this be the case and what implications does this have for education in the cyber domain?

First, an example in cybersecurity education: for a learner first presented with **nmap**, the network mapping tool, what does the blinking cursor invite? When the search begins, the learner no longer maintains a meaningful dichotomous distinction from the computer. While they may be *treating* the computer as alteric, the learner's machine itself recedes into the background as they beings to embody the interface, a **user-nmap** hybrid. Much as Ihde experiences the chalkboard through the chalk or Heidegger's carpenter experiences the nail through the hammer, the learner is experiencing the network landscape through the keyboard and screen, the capabilities of the software, and their familiarity with each system involved. We can now see the range of postphenomenological components at play: the multistability (computer-as-productivity-tool versus computer-as-attack-surface) and transparency (the learner embodies the keyboard and the software) of the hardware. As in traditional phenomenological analysis, uncovering the hidden stabilities in the complex network of devices and intent can be prohibitively difficult. The process takes practice.

This difficulty (or, optimistically, opportunity) is partly due to the lack of any "strict postphenomenological methodology that scholars could follow. Postphenomenology comes in just as many flavors as there are scholars in the field" (Rosenberger & Verbeek, 2015, p. 2). This results in an openness allowing cybersecurity researchers and educators to explore the possibilities presented here. Variation and multistability in the world of cybersecurity is ever-present: a website exploit is a prime example. A feature in a website with a particular intended function can be used for something unintended,

often nefarious. The phrase, "It's a feature, not a bug" is itself a description of a technology's multistability and a reflective breakdown analysis. Postphenomenological tools like variational analysis are key in uncovering not just multistabilities, but even revealing the technologies, themselves. Teaching learners to approach the cyber domain with these relations in mind can help them engage in "phenomenological looking" (Ihde, 2012), unveiling experiences they are having but unaware of.

Returning to the K12 Cybersecurity Standards Learning Standards (2021), we see how one might use postphenomenological methods to explore and instruct. Concretely, **K-2.DC.THRT**, "Describe good and bad uses of digital devices" is precisely a variational analysis. Consider how photography is specifically identified in the gradeband standard: variational analysis of this leads to the revealing of photo "tagging" on social media as both a space for community building and memory-making, while also potentially being a place for ridicule, ostracization, or harassment (for detailed examples of this approach, see Rosenberger (2020) for bench-as-library and bench-as-political-statement). Similarly, the "Digital Footprint" standards like **6-8.DC-FOOT.2**, "Recognize the permanence of a digital footprint," suggests "digital heaviness" (O'Neal Irwin, 2018), a weight felt when private moments are digitally exposed publicly.

8. LIMITATIONS

While taking a postphenomenological approach to the cyber domain and cybersecurity education may indeed expose new concepts, experiences, and considerations, the methodology is not without its limitations. Primarily, the practical application of postphenomenological methods can be a significant hurdle for educators and researchers.

Postphenomenology has been criticized for lacking a mechanism to explore systemic issues and instead focusing entirely on individualized experience. Arzroomchilar (2022) draws attention to the postphenomenological tendency to ignore the historical context of a technology and the "debates, disputes and fights" (np.) accompanying it, as well as the omission of social and political analyses inherent in the framework. Aagaard (2017) likewise points out the range of feminist critiques and responses in the literature surrounding issues of the politicization of experience and the natural discourse surrounding the use of technologies. Especially in the cyber

domain, future research and analysis into these critiques would provide a more robust framework.

9. CONCLUSION

In the preceding pages, I have attempted to draw meaningful connections between traditional phenomenology, the technologically focused postphenomenology, ways one may "do" postphenomenology in the cyber domain, and the need for and application of those methods in cybersecurity and cybersecurity education. While there is no hard-and-fast walkthrough for engaging in a postphenomenological study, I have presented a variety of methods to apply and tools to use, most notably those of variational analysis to reveal a technology's multistability, and the prereflective and reflective approaches of the postphenomenology of practice. Examples of postphenomenological studies have also been highlighted along with criticisms and suggestions for future study.

This leaves avenues to explore. The most relevant to cybersecurity and cybersecurity education may be that of the present understanding and confines of the complex intentionalities involved. Within the cybersecurity domain, it's entirely possible the postphenomenological intentionality landscape may need expanded to account for common situations like on-path attacks (a "sabotage intentionality," perhaps, to describe the injection of a bad actor's intent into a victim's experience). This is precisely why postphenomenology may prove exceedingly fruitful in cybersecurity education: focusing on the potentially conflicting intentionalities and mediations present in the cyber domain may make possible the moving beyond what is often a transactional and purely technical venture. Some, like Blair et al. (2020) and Austin (2020), point explicitly to the need for wholesale reconsideration of the nature of cybersecurity education, suggesting the need for—in contrast to the frequent autodidacticism seen presently—holistic and institutional research-based approaches, respectively. Crucially, a postphenomenological approach may be a solution to Blair et. al.'s challenge that "cyber should also be addressed when covering most of the social sciences (such as political science, economics, international relations, and sociology) as well as in law, ethics, and social justice components, and in studies of human behavior" (p. 5), given the infusion of technology into all spaces.

In fact, there is no shortage of opportunities to apply a postphenomenological approach to

cybersecurity and cybersecurity education: one could delve deep into competitions held by various cybersecurity organizations like the National Cyber League, explore spam email and what we can learn about how it is experienced differently between users, perform variational analyses in a penetration testing course on any of the range of software bundled in Kali Linux. If technology is involved, researchers and educators may attempt applying postphenomenology to uncover those heretofore unseen stabilities.

As such, this paper is intended to build a foundation for postphenomenological explorations into the cybersecurity and cybersecurity education domains. Of particular and timely importance is the sudden and ubiquitous appearance of generative AI like ChatGPT (OpenAI, 2023) and the extraordinary ways this technology will influence all domains, not just those discussed here. For example, the recent release of WormGPT, a “blackhat alternative” to ChatGPT and other generative text systems (WormGPT, 2023), presents a meaningful and worthwhile subject for postphenomenological analysis. Future research is invited to further act on the postphenomenological approach and find the as-yet unseen ways these technologies influence more than just education.

10. REFERENCES

- Aagaard, J. (2017). Introducing postphenomenological research: A brief and selective sketch of phenomenological research methods. *International Journal of Qualitative Studies in Education*, 30(6), 519–533. <https://doi.org/10.1080/09518398.2016.1263884>
- Adams, C., & Turville, J. (2018). Doing Postphenomenology in Education. In J. K. B. Friis, J. Aagaard, J. Sorenson & O. Taldrup (Eds.), *Postphenomenological Methodologies: New Ways in Mediating Techno-Human Relationships* (pp. 3–25). Lexington Books.
- Arzroomchilar, E. (2022). Some Suggestions to Improve Postphenomenology. *Human Studies*. <https://doi.org/10.1007/s10746-021-09615-1>
- Austin, G. (2020). Twelve dilemmas of reform in cyber security education. In G. Austin (Ed.), *Cyber Security Education*. Routledge.
- Ayas ÖnoI, T., & Akyaman, S. (2021). “What’s The Point of Exercising If It Cannot Be Measured?” A Post-Phenomenological Analysis of Self-Tracking Devices. *AGATHOS*, 12(2), 7–23. https://www.agathos-international-review.com/issue12_2/03.Onol%20&%20Akayaman.pdf
- Besmer, K. (2012). Embodying a Translation Technology: The Cochlear Implant and Cyborg Intentionality. *Techné: Research in Philosophy and Technology*, 16(3), 296–316.
- Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In G. Austin (Ed.), *Cyber Security Education*. Routledge.
- Blitz, M. (2014). Understanding Heidegger on Technology. *The New Atlantis*, 41, 63–80.
- Chiosea, F. (2020). *The State of Cybersecurity Education in K-12 Schools*. EdWeek Research Center. <https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf>
- Cyber Innovation Center, & CYBER.ORG. (2021). *K-12 Cybersecurity Learning Standards*. <https://cyber.org/standards>
- Gutland, C. (2018). Husserlian Phenomenology as a Kind of Introspection. *Frontiers in Psychology*, 9.
- Heidegger, M. (1927). *Being and Time* (2010 translation). State University of New York Press.
- (ISC)². (2022). *(ISC)² 2022 Cybersecurity Workforce Study*. <https://www.isc2.org/Research/Workforce-Study>
- Ihde, D. (1990). *Technology and the Lifeworld: From Garden to Earth*. Indiana University Press.
- Ihde, D. (2003). Postphenomenology - Again? *Working Papers from the Centre for STS Studies, University of Aarhus*, (3).
- Ihde, D. (2012). *Experimental Phenomenology: Multistabilities* (2nd ed.). State University of New York Press.
- Irwin, S. O. (2018). The Unbearable Lightness (and Heaviness) of Being Digital. In A. Romele & E. Terrone (Eds.), *Towards a Philosophy of Digital Media* (pp. 185–203). Springer International Publishing.
- Lynch, J., Hughes, G., Papoutsis, C., Wherton, J., & A’Court, C. (2022). “It’s no good but at least I’ve always got it round my neck”: A postphenomenological analysis of reassurance in assistive technology use by

- older people. *Social Science & Medicine*, 292, 114553.
<https://doi.org/10.1016/j.socscimed.2021.114553>
- Majkut, P., Carrillo Canan, A. J. L., Basch, C. A., Conde, O., Dalke, T. P., Egan, K. S., Borup, T., Bourdaa, M., & Cline, K. (2009). On deception: A phenomenological approach. In P. Majkut & A. J. L. Carrillo Canan (Eds.), *Deception: Essays from the Outis Project on Deception*. Zeta Books.
- Moran, D. (2000). *Introduction to Phenomenology*. Routledge.
<https://arxiv.org/abs/0712.0689>
- Morrison, L. A. (2020). Situating Moral Agency: How Postphenomenology Can Benefit Engineering Ethics. *Science & Engineering Ethics*, 26(3), 1377–1401.
<https://doi.org/10.1007/s11948-019-00163-7>
- OpenAI. (2023). *ChatGPT*.
<https://chat.openai.com>
- Pinchot, J., Cellante, D., Mishra, S., & Poullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal (ISEDJ)*, 18(3), 44–53.
- Rosenberger, R. (2009). The habits of computer use. *International Journal of Computing & Information Technology*, 1(1), 22–28.
- Rosenberger, R. (2020). On variational cross-examination: A method for postphenomenological multistability. *AI & SOCIETY*. <https://doi.org/10.1007/s00146-020-01050-7>
- Rosenberger, R., & Verbeek, P.-P. (2015). A Field Guide to Postphenomenology. In R. Rosenberger & P.-P. Verbeek (Eds.), *Postphenomenological Investigations: Essays on Human-Technology Relations* (pp. 9–41). Lexington Books.
- Van Manen, M. (2014). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Left Coast Press.
- Verbeek, P.-P. (2008a). Cyborg intentionality: Rethinking the phenomenology of human-technology relations. *Phenomenology and the Cognitive Sciences*, 7(3), 387–395.
- Verbeek, P.-P. (2008b). Obstetric ultrasound and the technological mediation of morality: A postphenomenological analysis. *Human Studies*, 31(1), 11–26.
<https://doi.org/10.1007/s10746-007-9079-0>
- Verbeek, P.-P. (2015). Toward a Theory of Technological Mediation. In J. Kyrre Berg Friis & R. P. Crease (Eds.), *Technoscience and Postphenomenology: The Manhattan Papers*. Lexington Books.
- Verbeek, P.-P. (2023). Postphenomenology and Ethics. In *Technology Ethics*. Routledge.
- Wagner, P. (2023). CyberEducation-by-Design. *Cybersecurity Pedagogy and Practice Journal*, 2(1), 50. <https://cppj.info/2023-2/n1/CPPJv2n1p50.htm>
- Wellner, G., & Levin, I. (2023). Ihde meets Papert: Combining postphenomenology and constructionism for a future agenda of philosophy of education in the era of digital technologies. *Learning, Media and Technology*, 1–14.
<https://doi.org/10.1080/17439884.2023.2251388>
- Vindenes, J., & Wasson, B. (2021). A Postphenomenological Framework for Studying User Experience of Immersive Virtual Reality. *Frontiers in Virtual Reality*, 2, 656423.
<https://doi.org/10.3389/frvir.2021.656423>
- WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks*. (2023). The Hacker News.
<https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html>
- Zheng, E. L. (2021). Interpreting fitness: Self-tracking with fitness apps through a postphenomenology lens. *AI & SOCIETY*.
<https://doi.org/10.1007/s00146-021-0114>