# A University's Developmental Framework: Creating, Implementing, and Evaluating a K-12 Teacher Cybersecurity Micro-credential Course

**Bekir Mugayitoglu**
School of Teacher Education, University of Wyoming
Laramie, Wyoming 82071, USA

**Mike Borowczak**
Department of Computer Science, University of Wyoming
Laramie, Wyoming 82071, USA

**Andrea C. Burrows**
School of Teacher Education, University of Wyoming
Laramie, Wyoming 82071, USA

## ABSTRACT

At present, there is limited understanding of cybersecurity micro-credentials and their impact on K-12 teachers. This work evaluates a university's development of a computing-based learning and teaching environment for K-12 teachers, focusing on a set of cybersecurity micro-credential modules that we encapsulate within micro-credential professional development (PD) opportunities. This ongoing work consists of two pilot studies (Pilot 1 and Pilot 2) over an academic year (2020–2021) that engaged 21 K-12 teachers. The research questions explore the benefits and challenges of the cybersecurity micro-credential PD. The authors developed two modules for Pilot 1: Introduction to Cybersecurity (Module 0) and the Confidentiality, Integrity, and Availability (CIA) Triad (Module 1). There were nine K-12 teachers enrolled in the Pilot 1 course, with five participating in all aspects of the pilot study. The authors developed three more modules for Pilot 2: Abstraction (Module 2), Modularity (Module 3), and Least Privilege (Module 4). The authors utilized quantitative and qualitative data collection via four methods: 1) Assessment and lesson plan scores (quantitative); 2) thirteen semi-structured interviews (qualitative); 3) two bi-weekly progress reports (qualitative) and 4) two focus groups (qualitative). They assessed teachers' knowledge gains in specific cybersecurity and computing. The authors coded interview question answers, focus group notes, and bi-weekly progress report summaries and grouped them into major themes by searching descriptive words. This research study showcases innovative tools (i.e., micro-credential modules) for teaching cybersecurity. Lastly, the authors describe a method to deliver cybersecurity content through a micro-credential based on virtual PD for K–12 teachers. The main limitation in this work is the small sample size.

**Keywords**: Computer Science, Cybersecurity, Cybersecurity Education, Micro-credential, Virtual Professional Development, K-12 Teacher, School Districts

## 1. INTRODUCTION

Teaching cybersecurity can be a difficult and overwhelming process for K-12 teachers, which requires fundamental content knowledge, pedagogical content knowledge, and understanding in a wide range of topics. Not many K-12 teachers synthesize and integrate cybersecurity content knowledge into their K-12 classroom environments [1]. The authors believe that engaging with cybersecurity, principles of cybersecurity, and computing education enables K-12 teachers to not only learn content, but also to educate their students in cybersecurity. The authors, K-12 teacher practitioners, educational experts, and computer science experts developed, created, and implemented a university-supported computing-based learning and teaching online environment to teach cybersecurity. There was an emphasis on creating a high-quality micro-credential. The micro-credential professional development (PD) was created with the purpose to prepare K-12 teachers to be confident teaching cybersecurity principles and allow them to empower their students to be fluent in cybersecurity. It is important to recognize that while a set of micro-credentials might resemble a course in combined length, the modules we have created are not a course and no credit is earned for taking the micro-credentials themselves. A training that prepares K- 12 teachers to teach new concepts in cybersecurity education is vital for computing education and cybersecurity habits.

[1] The authors are grateful to Dr. Trina Johnson Kilty for the editing of this article.

While there is no unified consensus, or universally accepted set of cybersecurity principles, this work focuses on 11 primary principles derived from the NSA GenCyber programs' Cybersecurity First Principles and Cybersecurity Concepts [2,3,4,5]. In reality, what constitutes fundamental cybersecurity principles varies based on which source one references, as several of these principles can overlap in places, or that some of these principles may be best considered as sub-ideas under other principles, but the authors of this paper have been operating under the idea that these are all distinct ideas. The authors accept that there is an amount of overlap between principles, but as the authors are working in a teaching environment, a field filled with repetition, the authors are openly embracing the overlaps, and using it as a latching-on point to cement connections between principles. Twelve can be partitioned into several individual units in order to group concepts and principles by core ideas. This takes into consideration the concern that some principles could be considered sub-ideas. The three units that the authors created were fundamentals (with a focus on introductory and base knowledge), philosophies (focused on abstraction and principles related to the abstraction process), and segmentations (focusing on the concepts related to keeping things separated). The authors debated whether modularity should be in philosophies or segmentations units but decided to leave it as the last unit in philosophies, both to keep the units equal in module size, and to ensure it was completed first in order to introduce the concept.

## 2. PROBLEM, PURPOSE, AND RESEARCH QUESTIONS

PD programs are not generally cost effective and can take time away from being in the classroom with students [6,7]. Often, the teacher must pay for their own PD, attend on their personal time, and the PDs are not specifically targeted at the knowledge needed [8]. These problems face many teachers acting as a self-advocate within their line of duty. In order to find free, online resources and computer science skill groups, teachers must dedicate a substantial amount of personal time to finding PDs where the credits are not necessarily transferable to a certification or count for continuing education credits. Micro-credential programs, like the gamified badge-based systems, seek to enable teachers to earn the educational credits that can transfer with them, wherever their future placements take them, thus reducing the disparity of work required to be redone at every new posting. Micro-credentials are an opportunity for an alternative credentialing source for each state and can be implemented into individual states' licensure systems [9,10,11,12]. While developing the cybersecurity micro-credential, the researchers added resources (e.g., videos, websites) and research (e.g., journal articles, conference papers, book chapters) to ensure they were up-to-date, content-rich, and comprehensible by the K-12 teachers.

These resources and research would provide K-12 teachers with the opportunity to gain experiences, accrue content knowledge and pedagogical knowledge in interpreting the types of graphs, figures, and models to implement in their classroom pedagogy. For example, the Data Talk website has classroom activities [13]. These activities consisted of topics and interactive ways to inform teachers about data analysis and allow them to implement in their classroom instruction. Additionally, Dynamic Data Science has a dynamic data set of lesson plans aligned with math standards and includes several lesson plans. This resource allowed teachers an opportunity with data set cleaning, sorting, and interpreting while receiving instant feedback [14].

For micro-credential programs to be effective, they must account for various forms of disparities [15]. For learning programs to be accessible to teachers facing disparities in costs, accessibility, gender representation, and a lack of diversity, programs must account for these disparities and seek out ways to be inclusive for these groups [16, 17]. Being inclusive is a driving goal for the micro-credential PD in cybersecurity. Wyoming's computer science content and performance standards have been recently adopted and contain cybersecurity principles [18]. The Wyoming computer science content and performance standards allows teachers to align their lesson plans and artifacts with standards. These standards were taken into consideration when developing the cybersecurity micro-credential. Each module of the cybersecurity micro-credential addresses one of the cybersecurity principles [2] and each principle includes sample lesson plans that incorporate the Wyoming computer science content and performance standards. Table 1 shows how this integration allowed teachers to align their lesson plans and artifacts on CIA Triad (Module 1) based on a variety of grade levels (K-2, 3-5, 6-8, and 9-12).

Table 1. The Wyoming Computer Science Content and Performance Standards that aligned with CIA Triad (Module 1)

| Module | Grade Level | Standard |
|---|---|---|
| The Confidentiality, Integrity, and Availability (CIA) Triad (Module 1) | K-2 | 2.NI.C.01 Explain what authentication factors (e.g., login) are, why we use them, and apply authentication to protect devices and information (personal and private) from unauthorized access. |
| | 3-5 | 5.NI.C.01 Discuss real-world cybersecurity problems and identify and implement appropriate strategies for how personal information can be protected. |
| | 6-8 | 8.IC.SLE.01 Using grade appropriate content and complexity, describe tradeoffs between allowing information to be public and keeping information private and secure. |
| | 9-12 (Level 1) | L1.NI.C.03 Compare various security measures, considering trade-offs between the usability and security of a computing system. |
| | 9-12 (Level 2) | L2.NI.C.01 Compare ways software developers protect devices and information from unauthorized access. |

This cybersecurity micro-credential PD discussed in this study developed a program that prepared K-12 teachers to teach cybersecurity principles. Specifically, the authors created and implemented a virtual PD experience for K-12 teachers, which was developed on Canvas Learning Management System. The purpose of the study was for the authors to develop understandings of the micro-credential qualities that K-12 teachers found beneficial and challenging. Working with recommendations to create PDs of high quality and providing the best experience possible for teachers facing inequalities, the authors provided the teachers opportunities for cybersecurity knowledge growth. All teacher learners were provided the same opportunities online which can diminish discrimination [19]. Thus, the authors sought to find what worked or did not work for the K-12 teachers as they engaged with the micro-credential PD module for iterative improvements.

**Research Questions**

1. How did the micro-credential module resources benefit K-12 teachers to build their cybersecurity knowledge?

2. Is there correlation between the K-12 teacher assessment scores and their total time in hours spent on micro-credential modules 0 and 1 (Pilot 1) and 0, 1, 2, 3, and 4 (Pilot 2)?

3. Is there correlation between the K-12 teacher lesson plan scores and their total time in hours spent on micro-credential modules 0 and 1 (Pilot 1) and 0, 1, 2, 3, and 4 (Pilot 2)?

4. What were the K-12 teacher perceptions of benefits and challenges with the cybersecurity micro-credential modules?

## 3. LITERATURE REVIEW

PD programs are sometimes not an effective way to train teachers and can include 1) K-12 teachers that do not have enough time in their teaching schedules to implement new techniques learned during PD courses, 2) PD programs that are short-term, 3) PD materials that do not allow K-12 teachers to make connections with their own teaching area and/or curriculum, and 4) K-12 teachers that have a chance to go through materials only during the PD programs [20]. However, high-quality and ongoing PD opportunities allow K-12 teachers to learn while educating their students, in particular, virtual PD programs, such as a micro-credential [9,10,11]. Micro-credentials are an effective way to enhance teachers' content and pedagogical knowledge to implement in their subject area. The micro-credential also provides K-12 teachers not only the ability to explore new concepts and practices during the micro-credential, but also after the micro-credential ended since the micro-credential provided e-materials that exist online (e.g., videos, articles, tools, journal articles). The longer duration of exploring also allows the K-12 teachers to become familiar with new teaching strategies, concepts, and practices, and to construct and retain new knowledge while going over the materials repetitively and integrating the ideas into classroom instruction [9,11].

Cybersecurity is important for K-12 teachers in the classroom to mold digital creators instead of digital consumers [21,22]. In other words, teachers can benefit from infusing the fundamentals of cybersecurity into their knowledge in the classroom. Teaching fundamentals empower students to apply cybersecurity principles and concepts in real-life while using technological devices. Additionally, it allows K-12 students to be cyber-literate instead of only interacting with technological devices while browsing the website or participating social media platforms without knowledge of cyberspace. However, there is a gap in cybersecurity education, in particular, K-12 teacher preparation in teaching cybersecurity [16]. Additionally, the 2019 State of Computer Science Education Equity and Diversity Report states that it will take many years to close the gap of computer science education [16,1]. One of the ways to close this gap is to provide K-12 teachers with access to computing and cybersecurity resources that align to the needs of their students, and our research study begins to fill this gap in the literature.

The EdWeek Research Center 2020 Report, *State of Cybersecurity Education in K-12 Schools: Results of a National Survey,* demonstrates that K-12 cybersecurity education is vital [23]. It states that K-12 student learners should know cybersecurity concepts, principles, and practices to protect themselves online and be prepared for the future. However, many students are not exposed to these concepts about cybersecurity because their teachers are not knowledgeable in cybersecurity methods, practices, and concepts. Stated differently, many students are not able to gain knowledge about cybersecurity if their teachers do not know about it. Interestingly, the report shows that on a survey with approximately 1000 educator participants, ninety one percent (91%) of K-12 teachers indicate that they know at least a little bit about cybersecurity while only ten percent (10%) know a lot. It could be argued that their students know less than the teachers. There is also an equity problem relating to poverty within school districts [16, 19]. Therefore, a gap exists to broaden K-12 teacher fundamental and advanced cybersecurity knowledge for all students. The authors provided fundamental principles of cybersecurity (e.g., abstraction, modularity, layering) and computing education in the created micro-credential PD modules.

Although cybersecurity and computing education is demanding in K-12 education, learning is occurring disproportionately in higher economic status schools versus lower economic status schools [16, 19]. As researchers know that cybersecurity PD practice is needed, particularly in underrepresented and lower economic status schools, the authors used this to guide the micro-credential PD module creation.

Even though there is a demand for cybersecurity education, even if it is often not explicit, the majority of K-12 teachers do not have the opportunity to access information to gain knowledge and teach their students cybersecurity for several reasons.

First, the majority of K-12 teachers are not qualified to teach cybersecurity and computing because of the lack of cybersecurity knowledge, resources, and skills [24, 25]. Therefore, teachers do not know where to start to integrate cybersecurity instruction into their classrooms for their students, particularly in lower economic status schools [23]. In addition, based on the previously mentioned report, eighty percent (80%) of K-12 teachers mentioned that there are no cybersecurity resources in rural lower economic status schools. Based on this report and others [23] cybersecurity resources are crucial for K-12 teachers, in particular, public, high-poverty schools/districts. In summary, there is also a lack of K-12 teachers knowledgeable about cybersecurity topics because of a lack of accessibility to resources.

That cybersecurity is not often taught as a standalone course could be due in part to this lack of teaching knowledge combined with lack of resources. Moreover, the report also indicates that cybersecurity is often not taught as a course, but only as a part of the computer science classes. The cybersecurity topics that students learn from K-12 teachers are only the topics such as cyberbullying/cyberterrorism and basic digital literacy.

The following seven principles must be present in order for PD to be high quality. The micro-credential PD coined by Loucks-Horsley's seven principles that focus on 1) learning transparency, 2) broadening opportunities for teachers to reflect on pedagogical practices 3) encouraging teachers to shape learning communities with other STEM teachers,4) facilitating leadership among teachers, 5) teaching or linking between STEM teachers as common to efficient PD experiences for STEM teachers [20, 26].

## 4. METHODS

The cybersecurity micro-credential research team (including the authors) recruited nine K-12 teachers for the Pilot 1 study, with five teachers ultimately completing all components of the PD and study. Participants were tasked with completing the first two modules of cybersecurity fundamentals, which included an "Introduction to Cybersecurity" and "The CIA Triad." By limiting the pilot to only the first two modules, the teacher participants required four weeks to complete the required deliverables. The Pilot 2 study included five modules (0-4) titled Module 0 (Introduction to Cybersecurity), Module 1 (CIA Triad: confidentiality, integrity, and availability), Module 2 (Abstraction), Module 3 (Modularity), and Module 4 (Least Privilege). There were 16 teachers that were recruited who, based on the required deliverables, completed Pilot 2 within the six-week timeframe of the study.. For both pilot studies (Pilot 1 and Pilot 2), quantitative and qualitative data was collected and included 1) Assessment scores (quantitative); 2) semi-structured interviews (qualitative); 3) bi-weekly progress reports (qualitative) and 4) focus group (qualitative).

The Pilot 1 and Pilot 2 studies began with a virtual, introductory meeting where the authors explained the scope of the pilot to the participants. Following this meeting, the participant teachers were given access to the Learning Management System (LMS), Canvas, to access the cybersecurity modules.

The authors gathered data in the form of five semi-structured interviews, one focus group, and two bi-weekly progress reports between July 1 to July 28 in the Pilot 1 study. The authors gathered data in the form of eight semi-structured interviews, one focus group, and two bi-weekly progress reports between November 20 to December 31 in the Pilot 2 study.

Participants interacted with various information delivery formats through the LMS alongside completing the virtual assessments and quizzes. Various resource formats were used for information delivery including websites, journal articles, and videos. The participants completed one quiz for each module that served as a formative assessment. These quizzes were offered for participants and authors to monitor progress through the micro-credential without impacting final grades. Additionally, participants were expected to complete a bi-weekly progress report at the end of each module wherein they provided feedback on the overall layout and usability of the module. Finally, participants were given a variety of assessment formats to choose from for the final assessment of the CIA triad module. In addition to the participants being able to communicate and ask questions via email, the authors also scheduled weekly virtual office hours. These times were offered for participants to ask clarification questions, discuss topics with the authors and classmates, or simply as an opportunity to monitor individual understanding and progress through the modules. Finally, a virtual conclusion meeting was scheduled and conducted at the end of the four-week period of the pilot.

## 5. PARTICIPANTS

The K-12 teachers recruited for this study were not limited to one grade level or field of study. As such, the participants of Pilot 1 and Pilot 2 were from a variety of teaching fields and grade levels. Included in this study were STEM teachers, computer science teachers, and district technology specialists; grades taught by the participant teachers included elementary, middle, and high school levels. For Pilot 1, nine K-12 teachers enrolled to complete the modules, and five agreed to and participated in post-pilot interviews. In Pilot 2, there was a greater variety of teaching fields represented. Included in this study were computer science teachers, STEM teachers, math teachers, art teachers, English teachers, and library media specialists; grades taught by the participant teachers included elementary, middle, and high school levels. For Pilot 2, sixteen K-12 teachers enrolled to complete the modules, and eight agreed to and participated in post-pilot interviews.

K-12 teachers were categorized as computer science and non- computer science teachers based on their major, teaching experience, and endorsements. Most of the non-computer science teachers were science, technology, engineering, or mathematics (STEM) teachers. In Pilot 1, four teachers self-identified as a computer science teacher, and one identified as a non-computer science teacher. In Pilot 2, seven teachers self-identified as a computer science teacher, and nine identified as a non-computer science teacher.

In Pilot 1, based on how K-12 teachers self-identified on the demographic survey, 60% of participants were White, 20% of participants were Native American, and 20% of participants were Scotch Irish. In Pilot 2, 74% of participants were White, 13% of participants were Asian/Pacific Islander, and 13% of participants were Native American/American Indian. In Pilot 1 and Pilot 2, 71% were White, 14% of participants were Native American/American Indian, 10% of participants were Asian/Pacific Islander, and 5% of participants were Scotch/Irish.

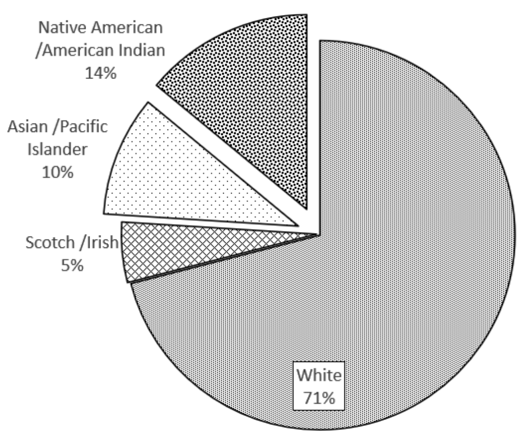


Figure 1. Percentage distribution of K-12 teachers' participation by race/ethnicity (Pilot 1 and 2).

As Figure 2 shows, there were more female participants (67%) than male participants (33%) in Pilot 1 and Pilot 2. There were more female participants than male participants during the four-week micro-credential pilot. There were three female K-12 teachers (60%), compared to two male K-12 teachers (40%) who completed the micro-credential PD. As Figure 2 shows, there were more female participants than male participants in Pilot 2 as well during the six-week micro-credential pilot. There were eleven female K-12 teachers (69%), compared to five male K-12 teachers (31%) who completed the micro-credential PD. The reports also support this disproportionate number of female and male participants [16, 17, 27].

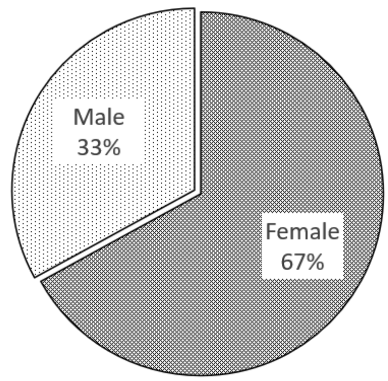


Figure 2. Percentage distribution of K-12 teachers' participation by gender (Pilot 1 and 2).

## 6. ANALYSIS AND FINDINGS

### Quantitative Research

Overall, quantitative results show that K-12 teachers with prior computer science/cybersecurity content and pedagogical knowledge tend to spend relatively less time to complete assessments and/or lesson plans since they already became familiar with the principles/modules. As Table 2 shows, bingo format assessment options were given after the completion of Module 0 materials, "Introduction to Cybersecurity," Module 1 materials, "The CIA Triad," Module 2 materials, "abstraction," Module 3 materials, "modularity," Module 4 materials, least privilege." It was clear from the assessment results that there was a connection between the completed assessment and the resources, supporting research papers, and essential vocabularies provided.

Table 2. Assessment Bingo: Bingo format for assessment options and choices.

| Papers | Short Papers | Tests | Other |
|---|---|---|---|
| Research Paper | Relation to Field | True/False | Teaching Video |
| Blog Post | Short Answer | Mixed Test | Explanatory Video |
| History Essay | Brochure | Write a Test | Presentation |

With a majority of the teacher participants identifying as white and there was racial underrepresentation and little diversity in the created micro-credential Pilot 1 & 2 PD which aligns well with the current computer science reports/cybersecurity reports and it is almost perfect racial representation in computer science/cybersecurity in K-12 [16,17]. As similar with K-12 students and teachers, computer science/cybersecurity is dominated by persons self-identifying as white [27].

In the quantitative research, the authors discovered a correlation between assessment scores and total time in hours spent on modules 0 and 1.

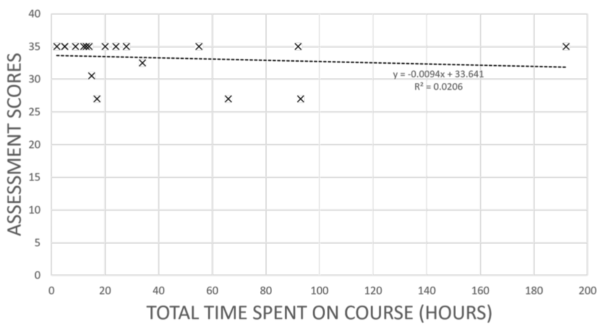


Figure 3. Assessment scores versus the total time in hours spent on micro-credential modules 0 and 1 (Pilot 1) and modules 0, 1, 2, 3, and 4 (Pilot 2).

Based on the learning management system analytics (Figure 3), Pearson's correlation coefficient was computed to assess the assessment scores and total time in hours spent on modules Pilot 1 and 2. There was a weak negative correlation between the assessment scores and total time in hours spent on module Pilot 0 and 1 ($r=-0.14$, $p<0.05$).

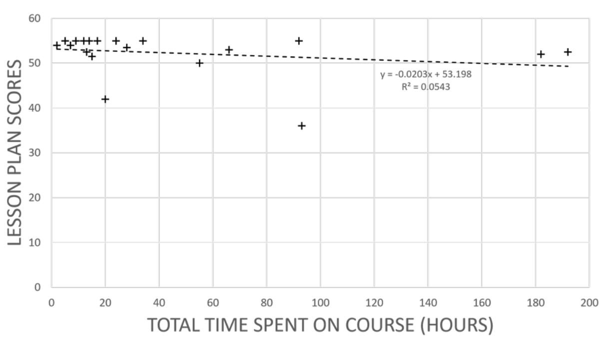


Figure 4. Lesson plan scores versus the total time in hours spent on micro-credential modules 0 and 1 (Pilot 1) and modules 0, 1, 2, 3, and 4 (Pilot 2).

Based on the learning management system analytics (Figure 4), Pearson's correlation coefficient was computed to assess the assessment scores and total time in hours spent on modules Pilot 1 and 2. There was a weak negative correlation between the assessment scores and total time in hours spent on module Pilot 0 and 1 ($r=-0.23$, $p<0.05$).

This result is evidence that computer science teachers already had prior knowledge in cybersecurity concepts and principles, therefore, they scored higher than non-computer science teachers, even though they spent less time in the micro-credential course modules. These computer science teachers could have possessed prior knowledge from cybersecurity teaching experience, computer science/cybersecurity certificates, or a major in computer science. Therefore, computer science teachers either did not watch/read or only partly watched/read resources, including videos, journal articles, and essential vocabularies. Data shows that non-computer science teachers' assessment scores were not as high as computer science teachers' assessment scores. This seems to indicate that the non-computer science teachers lacked background knowledge in computer science or cybersecurity or experience teaching computer science.

**Qualitative Research**

Overall, qualitative results show that resources (e.g., videos, websites, lesson plans) and research (e.g., journal articles, conference papers, book chapters) provided K-12 teachers to learn about the principles of cybersecurity so that they gained cybersecurity content and pedagogical knowledge. Therefore, these activities allowed K-12 teachers to use free, easy to understand and practical resources and research. In Table 3, K-12 teachers provided various comments regarding the positives and negatives of the micro-credential PD.

Table 3. Qualitative samples from four-week cybersecurity micro-credential showcasing quotes based on bi-weekly progress report and semi-structured interviews (From starting week one to end of week four) for K-12 teachers during Pilot 1 and from starting week one to end of the week six for K-12 teachers during Pilot 2).

| Pilot # | Days | Range of Week | Positive | Negative |
|---|---|---|---|---|
| Pilot 1 | 28 | Week 1 & 2 | "I thought the video choices were excellent." | "I am still not fully sure what you are looking from me as a pilot participant." |
| | | Week 3 & 4 | "I feel like I gained a better understanding of the differences between hackers." | "I read all of the...articles, they did not really add anything to my understanding." |
| Pilot 2 | 42 | Week 1 & 3 | "The articles were very helpful with explaining computational thinking in everyday examples along with giving activities pertaining to the module." | "One problem I had was creating a lesson that not to in depth. I kept adding and changing but I realized I needed to turn this into several lesson." |
| | | Week 3 & 6 | "I've had to teach all the teachers here how to use Canvas. It was fairly easy to get around for me. UW does a good job of putting those things together." | "I am not a great content reader, so I had trouble with those." |

In Pilot 1, spanning from the beginning of week 1 to the end of week 4, a few computer science teachers expressed that they liked the way that the videos and journal articles were embedded in the Canvas Learning

Management System. The videos were a short length, informative, and related to the pedagogical side of cybersecurity. Additionally, journal articles were provided with information related to the content-based technical and non- technical side of cybersecurity with tips and ideas. On the other hand, non-computer science teachers who had no prior computer science/cybersecurity knowledge were not able to build cybersecurity knowledge quickly enough to catch up to their computer science teacher peers and demonstrate their competency, even though they watched the videos more thoroughly than the computer science teachers.

In Pilot 2, spanning from the beginning of week 1 to the end of week 6, computer science and non-computer science teachers experienced various levels of difficulty based on the resources and journal articles presented (e.g., interactive flashcards, assessments). After providing the K-12 teachers with various materials, the positive comments showed clear benefits of flashcard use for computer science teachers and some even planned to utilize the flashcards in the classroom with their students. In particular, the flashcards were beneficial for computer science teachers in enriching and visually developing their cybersecurity content knowledge in the CIA triad. These results align well with previous findings and constructivist approaches as K-12 teachers were actively engaged and even created assessments such as brochures, presentations, and videos while using the content of interactive flashcards [28]. In particular, computer science teachers actively constructed their own cybersecurity content knowledge while activating their prior knowledge. On the other hand, flashcards and journal articles were not as helpful for non-computer science teachers. Besides, since non-computer science teachers lacked prior knowledge, they progressed more slowly, even though they received support from instructors via e-mail and weekly virtual zoom meetings. The previous evidence also indicates that novice teachers were not able to build knowledge as quickly or effectively as advanced computer science teachers due to a lack of scaffolding, prior knowledge, and structure based on the constructionism theory [29].

Several teachers expressed positive comments. One K-12 teacher commented, “I believe I can actually incorporate this into a day or two worth of the lesson. Maybe, even as many as three days into my beginning computer class.” While another K-12 teacher commented, “I think for schools that don’t have computer science this would be really beneficial for at least one of their teachers to have some experience with.” Several teachers expressed negative comments. One K-12 teacher commented, “I am just teaching K-6 I think cyber security the concepts as individual things like abstraction and modularity and least privileged in that type might be a little bit too advanced for my students.” Another K-12 teacher commented, “A lot higher thinking than elementary kids too so I mean those are great examples but then also you know simplifying it to how would you explain it to an elementary kid.”

Based upon the comments the K-12 teachers provided through the focus group, the overall consensus was that the micro-credential module resources were effectively organized relative to computer science content. Furthermore, the teacher participants felt that the information provided about cybersecurity created new pathways for their own learning and their teaching about online safety in their K-12 classrooms.

## 7. LIMITATIONS AND RECOMMENDATIONS

The main limitation in this work is the small sample size, but the contribution of development and evaluation methods help to set a research agenda for K-12 teacher preparation in cybersecurity. Besides, this work incorporated in Pilot 1 during only the four-week micro-credential pilot and Pilot 2 during only the six-week micro-credential. The authors will replicate the PD with additional modules, a longer duration, and more participants in the summer semester of 2021. This will in turn provide generalized results for a larger K-12 teacher population than those represented in this pre-pilot study.

There were many resources available, and K-12 teachers who were unfamiliar with cybersecurity may have been unsure where to begin or what to do during the micro-cybersecurity credential's material.

## 8. CONCLUSIONS AND APPLICATIONS

A research study with 21 participants, spanning two pilot studies (Pilot 1 and Pilot 2), was conducted to examine the effectiveness of PD in training computer science and non- computer science teachers to better implement computer science/cybersecurity topics in their classroom. Findings from the study showed that a short micro-credential based PD session can offer build up the computer science/cybersecurity content knowledge of computer science and non-computer science teachers alike. However, PD sessions often limit the amount of information that can be provided due to time limits of sessions. As such, the authors found that even intensive PD sessions cannot offer in-depth computer science knowledge to non-computer science teachers. From this information, the use of micro-credentials as an online curriculum delivery through modules could better prepare non-computer science teachers to incorporate computer science/cybersecurity topics in their classrooms.

According to the bi-weekly progress reports submitted by K-12 teachers, the majority of them were already familiar with the concepts in the cybersecurity principle because the CIA Triad is the fundamental introduction to cybersecurity. Additionally, K- 12 teachers were able to take the quizzes multiple times. In other words, they were retaking and going back to source materials to build their content knowledge. Even though the K-12 teachers had high scores, the assessments were not an accurate reflection of what the K-12 teachers learned. The K-12 teachers were engaged throughout modules 0 and 1 and interacted via email and even joined the virtual conference call meetings. There was a strong negative correlation between the assessment scores and total time in hours spent on module 0 and 1. A strong negative correlation indicates that non-computer science teachers' assessment scores were lower than computer science teachers' assessment scores even they spent more hours, potentially due to non-computer science teachers trying to learn a completely new content area and understand the new knowledge presented in modules 0 and 1.

The authors could conclude that providing a variety of options via the bingo format (e.g., teaching video, presentation, brochure) gave K-12 teachers opportunities to demonstrate what they have learned. Additionally, bingo format assessment options allow teachers to have an opportunity to create while personalizing a chosen assessment which can be meaningful and personalized teaching style for their students.

The findings from the modules support previous research determining that short-length videos are more beneficial for K-12 teachers because of decreased cognitive demand, and the short videos allowed the teachers to go back and re-watch the video again. The K-12 teachers watched a variety of videos which consisted of slides presented by an expert and/or animation. Teacher engagement and attention levels, especially those of computer science teachers, rose via the video instruction and scaffolded acquisition of content knowledge. Previous research demonstrates that teachers' high assessment scores, interviews, focus group responses, and bi-weekly progress reports support these findings [17, 30].

The results seem to indicate that computer science teachers with prior teaching experience and prior computer science knowledge tend to build knowledge more quickly and demonstrate competency more effectively than non-computer science teachers through online micro-credential PD  [29, 31].

The micro-credential demonstrated positive PD practices, such as consistency in the teaching, links through the PD, increased involvement of teachers and emerging teacher leaders. Researchers provided free, accessible, and high-quality resources and research to prepare teachers for the K-12 to educate the learners and to be teaching leaders in computer science/cybersecurity. K-12 teachers had an opportunity and flexibility to watch videos anytime and play, pause the video to watch repeatedly, shared the links and websites with their colleagues, and even implemented them in their classrooms the following day. K-12 teachers thus became teacher-leaders who would spread the cybersecurity resources (e.g., videos, websites) with other teachers such that not only computer science teachers but also STEM teachers can use as well.

K-12 Teachers developed their own learning network, in particular, when K-12 teachers who had already known one another and worked computer science and/or interdisciplinary fields (e.g., STEM). K-12 teachers were able to discuss insights with colleagues and organically continue collaboration while designing their lesson plans and/or creating their artifacts (e.g., presentations, brochures).

As authors continue working on K–12 cybersecurity education, they continue to investigate the kinds of supports that can enable K-12 teachers to successfully complete the micro-credential. In particular, the authors are excited to consider new iterations of online teacher PD to help teachers develop their own instructional materials and pedagogical content knowledge.

## 9. FUNDING

This work was supported by the Wyoming Department of Education (WDE) and the National Science Foundation (NSF) through the CS for All: RPP - Booting Up Computer Science in Wyoming (NSF Award #1923542) and Sustaining Wyoming's Advancing Reach in Mathematics and Science (NSF Award #1339853). Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF.

## 10. REFERENCES


[1] A. S. McCafferty & J. S. Beaudry, **Teaching Strategies That Creates Assessment-Literate Learners**, Corwin Press, 2018.

[2] National Security Agency GenCyber, **GenCyber CFP**.,p.3,2019.https://www.gencyber.com/proposals/rfp/gc-2019/

[3] National Security Agency Gencyber, **Program Director Guide**, 2016.

[4] B. R. Payne, T. Abegaz, and K. Antonia, Planning and Implementing a successful nsa-nsf gencyber summer cyber academy. **Journal of Cybersecurity Education, Research and Practice**, 2016.

[5] A. Burrows & M. Borowczak. CyberSecurity and Technology: How Do They Fit into a Science Classroom?. In K. Graziano (Ed.), **Proceedings of Society for Information Technology & Teacher Education International Conference** (pp. 2561-2569). Las Vegas, NV, United States: Association for the Advancement of Computing in Education (AACE). Retrieved from https://www.learntechlib.org/p/213831. 2019.

[6] D. E. Bartz and W. A. Kritsonis, **Micro-Credentialing and the Individualized Professional Development Approach to Learning for Teachers**, 2019.

[7] D. Herro, S. Arafeh, R. Ling, and C. Holden, **Mobile Learning: Perspectives on Practice and Policy**, IAP., 2018.

[8] D. Brown, **Research and educator micro-credentials.** Digital Promise, 2019.

[9] M. Borowczak, B. Mugayitoglu, A. C. Burrows, A., C. Kennedy, A. Carson, C. Person, & A. Finch. *Self-paced e-learning: Exploring the development of a cybersecurity micro-credential through K-12 teacher professional development.* **Paper presentation at the Society for Information Technology and Teacher Education Conference (SITE Interactive)**, Virtual. October 26, 2020.

[10] B. Mugayitoglu, M. Borowczak, A. C. Burrows, A. Carson, C. Person, A. Finch, & C. Kennedy. *A University's developmental framework: Creating, implementing, and evaluating a K-12 teacher cybersecurity micro-credential course.* **Paper presentation at the 12th International Conference on Education, Training, and Informatics (ICETI 2021)**, Virtual. March 9-12, 2021

[11] B. Mugayitoglu, A. C. Burrows, M. Borowczak, C. Person, A. Finch, C. Kennedy, & A. Carson. *Fostering accessibility: Creating high-quality, competency-based computer science micro-credentials for K-12 teachers*. **Paper presentation at the virtual Annual Meeting of the American Educational Research Association (AERA)**, Virtual. April 9-12, 2021.

[12] S. Wolf, A. C. Burrows, M. Borowczak, M. Johnson, R. Cooley, & K. Mogenson. **Integrated Outreach: Increasing Engagement in Computer Science and Cybersecurity.** *Education Sciences, 10*(12), 353. 2020.

[13] Stanford University. **Data Talks.** youcubed. Retrieved from https://www.youcubed.org/resource/data-talks/. 2021.

[14] The Concord Consortium. **Dynamic Data Science.** Retrieved from https://learn.concord.org/dynamic-data-science.

[15] J. Goode. **If you build teachers, will students come? The role of teachers in broadening computer science learning for urban youth.** *Journal of Educational Computing Research*, *36*(1), 65-88. 2007.

[16] Code.org, CSTA, and ECEP. **State of Computer Science Education Equity and Diversity.** 2019.

[17] J. Goode. Increasing Diversity in K-12 computer science: Strategies from the field. **In Proceedings of the 39th SIGCSE technical symposium on Computer science education** (pp. 362-366), 2008.

[18] **2020 Wyoming Computer Science Content & Performance Standards.** Retrieved from https://edu.wyoming.gov/wp-content/uploads/2020/07/2020-CS-WYCPS-07.10.20-for-SBE-Public-Input.pdf. 2020.

[19] J. Margolis, R. Estrella, J. Goode, J. J. Holme, & K. Nao, **Stuck in the shallow end: Education, race, and computing,** MIT press., 2017.

[20] S. Loucks-Horsle. ***Designing professional development for teachers of science and mathematics*.** Thousand Oaks, CA: Corwin Press. 2010.

[21] K. Brennan, A. Monroy-Hernández, and M. Resnick. Making projects, making friends: Online community as catalyst for interactive media creation, **New directions for youth development**, pp. 75-83, 2010.

[22] J. Ivy, et al., Seeding cybersecurity workforce pathways with secondary education, **Computer**, 52(3), pp. 67-75, 2019.

[23] EdWeek Research Center, **The State of Cybersecurity in Education in K-12 Schools**, 2020.

[24] M. Menekse, Computer science teacher professional development in the United States: a review of studies published between 2004 and 2014, **Computer Science Education,** 25(4), 325–350, 2015.

[25] M. R. Blanchard, C. E. LePrevost, A. D. Tolin, & K. S. Gutierrez, Investigating technology-enhanced teacher professional development in rural, high-poverty middle schools. **Educational Researcher**, 45(3), 207-220. 2016.

[26] S. Loucks-Horsley, N. Love, K. Stiles, S. Mundry, & P. Hewson. **Designing professional development for teachers of science and mathematics.** (2nd ed.) Thousand Oaks, CA: Corwin Press. 2003.

[27] Code.org, CSTA, and ECEP., **State of Computer Science Education**, Illuminating Disparities. 2020.

[28] E. Ackermann, **Constructionism in practice:**

**Designing, thinking, and learning in a digital world,** Routledge, 1996.
[29] S. Papert, I. Harel, Situating constructionism, **Constructionism**, 36(2), pp. 1-11, 1991.
[30] J. Kim, et al. Understanding in-video dropouts and interaction peaks inonline lecture videos, **In Proceedings of the first ACM conference on Learning@ scale conference,** (pp. 31-40), 2014.
[31] M. Ben-Ari. Constructivism in computer science education, **Journal of Computers in Mathematics and Science Teaching**, 20(1), pp. 45-73, 2001.