


12-2023

## EDUCATION AS A SOLUTION TO COMBAT RISING CYBERCRIME RATES AGAINST CHILDREN AND TEENAGERS

Christian Javier Solis-Diaz  
*California State University - San Bernardino*

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd>

 Part of the [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

---

### Recommended Citation

Solis-Diaz, Christian Javier, "EDUCATION AS A SOLUTION TO COMBAT RISING CYBERCRIME RATES AGAINST CHILDREN AND TEENAGERS" (2023). *Electronic Theses, Projects, and Dissertations*. 1811. <https://scholarworks.lib.csusb.edu/etd/1811>

This Project is brought to you for free and open access by the Office of Graduate Studies at CSUSB ScholarWorks. It has been accepted for inclusion in Electronic Theses, Projects, and Dissertations by an authorized administrator of CSUSB ScholarWorks. For more information, please contact [scholarworks@csusb.edu](mailto:scholarworks@csusb.edu).

EDUCATION AS A SOLUTION TO COMBAT RISING CYBERCRIME RATES  
AGAINST CHILDREN AND TEENAGERS

---

A Project  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

In Partial Fulfillment  
of the Requirements for the Degree  
Master of Science  
in  
Information Systems and Technology

---

by  
Christian Javier Solis-Diaz  
December 2023

EDUCATION AS A SOLUTION TO COMBAT RISING CYBERCRIME RATES  
AGAINST CHILDREN AND TEENAGERS

---

A Project  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

by  
Christian Javier Solis-Diaz

December 2023

Approved by:

Dr. William Butler, Committee Chair

Dr. Conrad Shayo, Committee Member, Chair, Department of Information and  
Decision Sciences

© 2023 Christian Javier Solis-Diaz

## ABSTRACT

Ninety seven percent (97%) of people between the ages of 3 and 18 are found to be users of technology and internet services daily. This number also correlates with rising cybercrime rates against people in this age bracket. It is found that people between 3 and 18 years old are found to be technologically savvy but often lack the knowledge of how to protect themselves in online environments. Researchers have suggested that cybersecurity awareness training is an effective method at combating common forms of cyberattack such as social engineering. Social engineering attacks are found to make up 98% of successful cyberattacks and it is crucial that users of these internet and technology services are knowledgeable in protecting themselves.

Cybersecurity education materials are commonly found in enterprise and higher education environments, but there is a gap of available research that evaluates the effectiveness of this education in the K-12 environment. Therefore, this project evaluates the following research questions to help address the gap: (Q1) What affective methods to educate children and teenagers on cybersecurity concepts? (Q2) What are best practices for topic selection when it comes to cybersecurity education in the 3–18-year age range? (Q3) What are unique challenges that may be encountered when implementing this type of education nationwide? The research will discover the answers for the proposed research

questions by analyzing existing literature and reviewing case studies of successful cybersecurity education in K-12 schools.

The selected case studies went through an inclusion and exclusion criteria which required the following items to be present: publishing by a reputable journal or conference, contain empirical data in form of pre and post assessment, why the method of teaching was selected, and explain limitations. The findings and conclusions from the case studies are: (Q1) Students are receptive to learning cybersecurity principles via multiple teaching styles. The case studies displayed self-guided, collaborative, and traditional instruction methods and students were shown to improve greatly in post assessment results. (Q2) Best practices for selecting topics in the case studies was to utilize age-appropriate cybersecurity educational materials published by government agencies. A finding from this is that these materials are not readily available for educators and must be sought out as they are considered optional items. (Q3) Scaling of these type of cybersecurity workshops is difficult due to resource constraints faced by many schools found in lower income and rural districts. The availability of cybersecurity professionals and university campus's willingness to host these camps is scarce and leaves this type of experience out of reach for many students. Areas of further study are researching methods on how to effectively scale this sort of education by utilizing a remote learning model and the creation of a standardized age-appropriate curriculum.

## ACKNOWLEDGEMENTS

I would like to acknowledge my friends and family for their ongoing encouragement and support throughout my graduate studies. I would like to personally thank my significant other, Cassandra Hernandez, for their ongoing support and encouragement at the most difficult moments of the project and for not allowing me to give up. Lastly, a sincere thank you to the committee members, Dr. Shayo and Dr. Butler, that devoted their time and provided support during this difficult process.

## TABLE OF CONTENTS

|  |      |
|--|------|
| ABSTRACT .....                                       | iii  |
| ACKNOWLEDGEMENTS.....                                | v    |
| LIST OF TABLES .....                                 | viii |
| LIST OF FIGURES .....                                | ix   |
| CHAPTER ONE: INTRODUCTION .....                      | 1    |
| Background of Study.....                             | 1    |
| Research Background .....                            | 6    |
| Problem Statement .....                              | 8    |
| Organization of Study .....                          | 9    |
| CHAPTER TWO: LITERATURE REVIEW.....                  | 10   |
| Effective K-12 Cybersecurity Education.....          | 12   |
| Cybersecurity Education Topics .....                 | 16   |
| Cybersecurity Education Challenges .....             | 18   |
| CHAPTER THREE: RESEARCH METHODOLOGY .....            | 22   |
| Selection of Research Articles .....                 | 22   |
| Methodology .....                                    | 23   |
| Selection of Case Studies.....                       | 25   |
| CHAPTER FOUR: CASE STUDY ANALYSIS AND FINDINGS ..... | 28   |
| Case 1: Cyber Aware.....                             | 30   |
| Attention.....                                       | 33   |
| Relevance .....                                      | 34   |
| Confidence.....                                      | 35   |



|  |    |
|--|----|
| Satisfaction .....   | 36 |
| Case 2: Penn State Berks.....  | 39 |
| Case 3: Visual Privacy Learning Tool .....   | 47 |
| CHAPTER FIVE: DISCUSSION, CONCLUSION, AND RECOMMENDATIONS<br>FOR FUTURE RESEARCH.....  | 55 |
| Question 1: What Are Effective Methods to Educate Children and<br>Teenagers on Cybersecurity Concepts?.....                                      | 55 |
| Question 2: What Are Best Practices for Topic Selection When It Comes<br>to Cybersecurity Education of People in the 3-18 Years Age Range? ..... | 56 |
| Question 3: What Are Unique Challenges That May Be Encountered<br>When Implementing This Type of Education Nationwide? .....                     | 57 |
| Conclusion .....   | 59 |
| REFERENCES .....   | 60 |

## LIST OF TABLES

|   |    |
|---|----|
| Table 1: Summary of Research and Relevant Publications .....  | 11 |
| Table 2. Participant Demographics (Yan et al., 2019). .....   | 15 |
| Table 3. Cybersecurity Education Inclusion and Exclusion Criteria .....                                   | 26 |
| Table 4. Summary of Jean Piaget’s Theory of Cognitive Development (Joubish & Khurram, 2011, p. 1262)..... | 28 |
| Table 5. Program Component Description .....  | 45 |

## LIST OF FIGURES

|  |    |
|--|----|
| Figure 1. Proposed Cybersecurity Curriculum (Javidi & Sheybani, 2019, p.4) ...                                       | 16 |
| Figure 2. Criteria for Healthcare Ransomware Articles (Adlaon, 2023, p.15). ....                                     | 27 |
| Figure 3. Cyber Aware ARCS Categories (Giannakas et al., 2019, p. 93) .....  | 33 |
| Figure 4: Mandatory Security Module (Giannakas et al., 2019, p 87). .....  | 34 |
| Figure 5. Relevance of Task Introduction (Giannakas et al., 2019, p.94) .....  | 35 |
| Figure 6: Visual Advancement (Giannakas et al., 2019, p.90) .....  | 37 |
| Figure 7: Scoring System (Giannakas et al., 2019, p.90) .....  | 37 |
| Figure 8. Summary of Cyber Aware Results (Giannakas et al., 2019, p. 99) .....                                       | 38 |
| Figure 9. Weeklong GenCyber Bootcamp Curriculum (Konak, 2018) .....  | 42 |
| Figure 10. Program Component in Hands-on Activity (Konak, 2018, p.7) .....   | 45 |
| Figure 11. Sample of Visual Privacy Application Interface (Chattopadhyay et al.2020, p.4).....                       | 48 |
| Figure 12. GenCyber Principles & Concepts Map: Visual-Privacy Learning Model (Chattopadhyay et al., 2020, p.5) ..... | 51 |
| Figure 13. Student Interest in Computer Science and Cybersecurity (Chattopadhyay et al., 2020, p.6) .....            | 52 |
| Figure 14. Sample Question and Participant Response (Chattopadhyay et al., 2020, p.8) .....                          | 53 |

# CHAPTER ONE: INTRODUCTION

## Background of Study

The use of technology and the internet around the world has increased drastically within the last few decades and has become the backbone to most of the services that people and organizations utilize every day. Researchers Li & Liu (2021) state that, "At present, most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace" (p. 1). It is estimated that over 65% of the world's total population has access to the internet and this number is steadily increasing year over year (Shewale, 2023). When grouping by age ranges, 33% of the reported users are reported to be between the ages of 3 and 18 years old (Laricchia, 2022). When narrowing the scope of these numbers to just the United States, 93% of adults are found to be users of both technology and internet services, while 97% of persons within between the ages 3 and 18 years old have access to both in some form as well (Vogels et al., 2022).

The adoption of technology and internet advancements have led to many benefits in society. For adults, technology and internet usage has brought forth improved productivity in the workplace, online services, and new jobs have been formed. Children and teenagers have benefited by increased accessibility to

information, improved problem-solving skills, and increased higher levels of motivation (Criollo-C et al., 2021). Although the benefits to technology adoption are numerous, there is one prevalent issue that has arisen that has affected businesses and people around the globe (Lopez, 2022; Morgan, 2022).

The increase of cybercrimes targeting information systems and their users has grown significantly with the adoption of technology and internet services. A study conducted by the Pew Research Center found that cyberattacks are a global threat comparable to climate change and terrorist attacks (Pew Research Center, 2019, p. 3). The increase can be attributed by the large financial incentives for malicious actors as cybercrime is estimated to be upwards of a 10 trillion-dollar industry by 2025 and expected to grow at a rate of 15% year over year for the foreseeable future (Morgan, 2022). Common forms of cybercrime involve taking advantage of the human element through methods of social engineering. Social engineering is defined as, "The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust (NIST, 2023, par. 1). According to Proofpoint (2023) social engineering attacks in some instances have success rates of 70% and account for 98% of total cyberattacks. As the success rates and costs of these cyberattacks are very high, organizations and individuals must be adequately informed on how to not fall victim to these attacks.

Children and teenagers in the previously mentioned age groups have become an emerging target for cyberattacks. As 97% of youth in the United States are found to be users of technology, this makes them a large vulnerable group (Vogels et al., 2022). Children and teenagers in this age range are often more likely to be technologically illiterate and may be more susceptible to falling for common online scams (Lopez, 2021). For example, The FBI Internet Crime Center Report from 2020 found that 3202 children fell victim to cybercrimes in 2020, increasing by 144% from the previous year (FBI, 2021). While children and teenagers are found to be exposed to technology at higher rates, as stated by Kuzmich (2019), “Young children are becoming more tech-savvy, they are not protection-savvy by nature and lack the understanding to know about the dangers that being online can present.”<sup>1</sup>. The human factor is crucial in preventing successful cyberattacks as social engineering methods circumvent technological safeguards. Foundational knowledge of cybersecurity concepts is essential in preventing common forms of cyberattacks that involve such tactics.

A case study conducted by Bullée et al. (2015) evaluated the cybersecurity awareness of students on a university campus. The main question asked during this research is, “To what extent are people susceptible to social engineering attacks?” (Bullée et al., 2015, p. 102). The researcher had a control group that has never been exposed to cybersecurity concepts and an experimental group who received information on the dangers of social

---

<sup>1</sup> <https://www.openaccessgovernment.org/children-vulnerable-to-cybercriminals/72665/>

engineering attacks a week before the experiment took place. The experimental group showed much higher performance by an average of 2.84 times over the control group. The case study shows that even in a short time, people who are exposed to cybersecurity concepts can drastically improve their knowledge of social engineering attacks. While similar case studies can be found in the university level or for the workplace, there is a gap of research that targets K-12 aged individuals (Javidi & Sheybani, 2019; Quayyum et al., 2021). Proposed reasonings behind the absence of literature are the lack of qualified individuals to teach these complex topics to students, the modernity of cybersecurity education, and lack of standardized curriculum for this topic (Javidi & Sheybani, 2019).

The implementation of such curriculum requires the involvement and support of multiple stakeholders within K-12 education. A stakeholder may be defined as, “An individual, group or organization that’s impacted by the outcome of a project or a business venture” (Landau, 2023, para. 2). In the context of education, the stakeholders may be students, parents, school staff, district staff, school boards, taxpayers, and the business community (RMC Research Corporation, 2009). Key stakeholders in education such as, the educators, district leaders, and principles often find themselves lacking the knowledge to adequately provide this type of education to students or in some cases completely lack any knowledge of the topic (Cyber Innovation Center, 2020). Factors that lead to this may be the geographic location and funding levels of the

school districts. As stated by the survey results by the Cyber Innovation Center, (2020):

Levels of educator knowledge vary significantly by work setting and professional role. Higher levels of knowledge are reported by private school employees, administrators, and educators in communities with cybersecurity resources. By contrast, lower levels of knowledge are reported among classroom teachers, in public schools, and in communities without cybersecurity resources such as cybersecurity companies, organizations that employ cybersecurity specialists, and universities that offer cybersecurity programs and/or conduct cybersecurity research. (p. 3)

From this open access survey, we can gather that many of the key stakeholders in the K-12 setting do not have the adequate knowledge or resources to begin a cybersecurity initiative at this grade level. When looking at the outside stakeholders such as the general population of students, parents, taxpayers, and the business community, much of the same sentiment is shared. A survey of internet users conducted by Olmstead and Smith (2017) found the median number of correspondents to answer only 5 out of the 13 cybersecurity comprehension questions correctly. The sample size used in this survey was 1,055 adults from different regions and backgrounds in the United States. The researchers attribute these lacking numbers to numerous factors but found the level of education was a key factor. As it was found that the respondents with



higher levels of education (bachelor's degree or higher) scored on average of 5.5 questions correctly while the group without higher levels of education scored on average 4.0 questions correctly (Olmstead & Smith, 2017). From both surveys, we gather that the main stakeholders in education are not educated around cybersecurity and those that are, come from more affluent school districts or areas around the country. From this, it was concluded that opinions from subject matter experts in cybersecurity such as educational institutions and industry professionals will need to be utilized to create a successful future for cybersecurity in the K-12 school system.

### Research Background

As there is a lack of literature available relating to the education of K-12 aged children on cybersecurity topics, ChatGPT 3.5 (Generative Artificial Intelligence) was utilized to narrow the scope of this research project. The following statement was input into the search engine, "What are further areas of research relating to educating K-12 aged students on cybersecurity concepts to prevent them from falling victim to social engineering attacks." Further areas of study suggested were the implementation of gamification and implementation of interactive learning methods that may be found enjoyable by students, curriculum development that may be utilized in the classroom, and the investigation of cybersecurity case studies of the named age ranges (OpenAI, 2023).

The research project will make use of case studies of cybersecurity education programs that are publicly available via the Google Scholar and OneSearch engines. Once chosen, the selected case studies will be used to analyze the efficacy of the delivery strategies and examine the material that was presented to determine whether the programs were found to raise students' understanding of common cyber-attacks. This method of research is chosen due to the recommendation by researchers calling for the evaluation of case studies (Yan et al., 2019; Rahman et al., 2020). For example, a systematic literature review conducted by Rahman et al., (2020), called the need for this type of education as K-12 aged children are at risk of cyberattacks due to rising technology usage and internet activity. The literature review concludes that cybersecurity education in the K-12 age range is vital and recommends investigation of security awareness programs suited for students (Rahman et al., 2020). Similar sentiment also found to be an area of further study in research by Yan et al., 2021. The research investigated the learning outcomes of participants of the GenCyber program. The scope of this research focused on nationwide GenCyber programs hosted at various universities around the country and took a quantitative approach to review intuitive and rational risk judgements portrayed by students before and after participation. As this research was broad, the researcher recommended a future area of investigation to focus on analyzing findings in a small subset of programs and focus on the underlying mechanisms that lead to success.

## Problem Statement

Technology and internet services have seen drastic increases in usage by users of all age groups. While the adoption of technology has shown to have incredible benefits, these benefits have introduced a new area of risk that a large majority of the population are unaware of. Risks such as cyberattacks have drastically increased due to the monetary incentives seen by malicious actors. A recent and emerging target for cybercriminals has been children and teenagers in the age ranges of 3-18 years of age (Tsirtsis et al., 2016). Persons within this age range have little resources when it comes to being educated in the topic of cybersecurity and has proven to become a growing worry as the numbers of cyberattacks against people this age have increased dramatically in the previous years.

Given the areas of future research suggested by previous researchers and ChatGPT 3.5, the outstanding research questions are:

1. What are effective methods to educate children and teenagers on cybersecurity concepts?
2. What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?
3. What are unique challenges that may be encountered when implementing this type of education nationwide?

## Organization of Study

This project is organized as follows: Chapter one introduced the problem. Chapter 2 will be a literature review. Chapter 3 is the project methodology and data collection. Chapter 4 is an analysis of the case studies. Chapter 5 is a discussion of the findings and areas for further study.

## CHAPTER TWO: LITERATURE REVIEW

*What are effective methods to educate children and teenagers on cybersecurity concepts?*

The research for the project was conducted primarily utilizing the Google Scholar search engine and supplemented by the California State University OneSearch tool. The search parameters for the project were set to peer reviewed articles and publications from the years 2010-2022. This allows for the information found to be up to date with the latest trends. The Google Scholar search engine allows the user to search for scholarly literature and ranks the articles by weight, publication, author, and number of citations (About Google Scholar, n.d.). Alternatively, the OneSearch tool provided by CSU is a search engine that provides access to library content found in the CSU catalog such as databases, books, and media (John M. Pfau Library, 2022). Additionally, information from organizations within the cybersecurity and education field were utilized if the information was found to be relevant to aid in answering the research questions. A summary of the articles selected will be provided in Table 1.

Table 1: Summary of Research and Relevant Publications

| Database Source                       | Search Terms                           | Search Results | Selected Publications | Authors   |
|---------------------------------------|--|----------------|-----------------------|---|
| Default / Google Scholar / One Search | Effective K-12 Cybersecurity Education | 4,190          | 30/4                  | <ul style="list-style-type: none"> <li>• (Domeji, 2019)</li> <li>• (Dawson et al., 2022)</li> <li>• (Yan et al., 2021)</li> <li>• (Javidi &amp; Sheybani, 2019)</li> </ul>    |
| Default / Google Scholar              | Cybersecurity Education Case Study     | 5,430          | 25/3                  | <ul style="list-style-type: none"> <li>• (Giannakas et al., 2019)</li> <li>• (Konak, 2018)</li> <li>• (Chattopadhyay et al., 2020)</li> </ul>                                 |
| Default / Google Scholar / One Search | Cybersecurity Education Challenges     | 2,510          | 15/4                  | <ul style="list-style-type: none"> <li>• (Rahman et al., 2020).</li> <li>• (Triplett, 2023)</li> <li>• (Nakama et al., 2018)</li> <li>• (Prior &amp; Renaud, 2022)</li> </ul> |

## Effective K-12 Cybersecurity Education

The first question to be answered is, “*What are effective methods of educating children and teenagers on cybersecurity concepts*” Therefore, the first keywords utilized in the literature review were “K-12 Cybersecurity Education” in the Google Scholar and CSUSB One Search engine. These search terms allowed for a holistic overview on the current landscape of educating K-12 aged individuals in cybersecurity concepts. It was found during the research process that specific word searches provided zero relevant articles or provided articles with zero relevancy to the project research questions. The lack of relevant literature is a sentiment shared by the research in the articles that will be discussed in the following paragraphs (Domeji, 2019; Javidi & Sheybani, 2019).

To begin, the first relevant article to the project was research conducted by Domeji (2019) which found the landscape of cybersecurity education lacks any form of structure or standardized curriculum and is found to be implemented in sporadic ways. This research attempts to create a theoretical framework for cybersecurity education that may be implemented by K-12 schools. By using a quantitative approach, the researcher was able to utilize survey results from numerous cybersecurity programs across the United States to address key findings of each program, such as the resource requirements, facilitators (Teachers, IT Staff, Online Resources), and participant ages. The limitations of this study were the broad scope of the programs and being unable to gather information on individual problems and how they were managed. A key finding

from the study was that cybersecurity education is typically delivered by a specialized instructor or a subject matter expert and found that in the surveyed programs, teachers were not equipped to instruct on these topics (Domeji, 2019).

The limitation of teacher knowledge on cybersecurity concepts is further explored by Dawson et al. (2022) in research that delves into the implementation of cybersecurity education in teaching credential programs due to the rise of cyber incidents K-12 institutions. This research suggests that K-12 teachers' exposure to cybersecurity concepts is almost nonexistent and levels of cybersecurity knowledge in surveyed instructors is found to be like surveys conducted a decade ago (Dawson et al., 2022). The solution presented in this research is to create a repository of curriculum created for educators in collaboration with cybersecurity experts that may be part of a teacher curriculum or a micro credentialing program (Dawson et al., 2022). The information can then be utilized by the educators to create sample lessons related to cybersecurity concepts that may be integrated to everyday learning. This research provides an example issue that may be problematic with long term implementation in classrooms as the execution of such credentialing programs will require the involvement of educators and security experts around the country. Considering this, the credentialing program discussed in this research may be a good beginning to closing the gap and allowing for teachers to feel comfortable teaching cybersecurity to their students.



A large study of rational and intuitive judgment of K-12 students and teachers was conducted by Yan et al. (2019). In this study, intuitive judgement was defined as, “An individuals’ capacity to examine evidence and make evaluations” (Yan et al., 2019, p.2) while rational judgement was defined as when, “Thinking is slow, effortful, rule-based, deliberately controlled and involves logical, hierarchical, and casual mechanical processes” (Yan et al., 2019, p.2). In the context of this research study, the researcher was evaluating the effectiveness of 45 GenCyber camps that were hosted in the United States, and the goal was the evaluate cybersecurity judgement of the participants to see if exposure to cybersecurity concepts improves risk-based judgement. The GenCyber research participants completed a survey before and after they participated in the GenCyber bootcamps. The demographics in this research covered were elementary, middle, high school, and respective teachers. A detailed figure containing the demographics of this study will be found in Table 2. The research findings were as follows: (a) Elementary school students are the highest risk group. (b) The region in which the bootcamp was conducted was found to be a risk factor as students from West and South regions of the United States scored significantly worse than their Northeastern counterparts. (c) More experience in GenCyber bootcamps does not equate to higher levels of understanding when it comes to cybersecurity topics.

Table 2. Participant Demographics (Yan et al., 2019).

| Age Group         | Pre-Assessment Survey Participant Count | Pre-Assessment Participant Percentage | Post-Assessment Survey Participant Count | Post Assessment Participant Percentage |
|-------------------|---|---------------------------------------|--|--|
| Elementary School | 224                                     | 8.3                                   | 0  | 0                                      |
| Middle School     | 696                                     | 25.7                                  | 177                                      | 17.3                                   |
| High School       | 1225                                    | 45.3                                  | 564                                      | 55.2                                   |
| Teacher           | 542                                     | 20.1                                  | 256                                      | 25.1                                   |
| Missing           | 16                                      | .6                                    | 24                                       | 2.4                                    |

While exposure to cybersecurity concepts provided positive outcomes for many of the participants, the researcher mentions a limitation of this study to be the broad scope and recommends evaluation of individual programs that target K-12 students.

Research by Javidi & Sheybani (2019), investigated the need for cybersecurity education in K-12 schools. The research suggests that there is a current shortage of qualified educators with the ability to educate students in computer science and cybersecurity related topics (Javidi & Sheybani, 2019). The researcher suggests that cybersecurity education in this age range is a community effort that will require involvement of, “teacher, parent, and the

community leaders alongside the students” (Javidi & Sheybani, 2019, p.3). The researcher suggests a cybersecurity curriculum based on six principles found in Figure 1. While the scope of this research was centered on providing the curriculum, the researcher calls for future endeavors to outline the curriculum in and conduct a real-world case study.

- 1. Academic and technical rigor**
- 2. Authenticity**
- 3. Applied learning**
- 4. Active exploration**
- 5. Adult connections**
- 6. Assessment practices**

Figure 1. Proposed Cybersecurity Curriculum (Javidi & Sheybani, 2019, p.4)

### Cybersecurity Education Topics

The second question to be answered for the culminating experience project is *“What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?”*. To understand the best practices for topic selection, the research will utilize case studies of cybersecurity education programs in K-12 schools. As previously mentioned, the learning strategies and topics covered may vary between younger and older students. Therefore, a real-world overview of how the topics were selected will

provide information to support a final recommendation. To find supporting articles, the following search terms utilized in the literature review were “Cybersecurity Education Case Study”. This search was conducted in the Google Scholar search engine. Once the parameters outlined in the previous search were placed, a total of 5,430 related articles were returned. A total of three articles were found to be relevant to the research project. Criteria for selection of the case studies is detailed in Table 2.

The first case study selected was conducted by Giannakas et al. (2019). The case has a target demographic of elementary aged students that introduces the students to a cybersecurity game application named CyberAware. This platform has a multitude of cybersecurity concepts that are delivered through a game content platform. The content delivery of this case study is through a gamified platform that has many tools and tips as the participants complete the challenges. This is a single player game that does not have any instructor led training or opportunities to collaborate with classmates. In terms of assessments, CyberAware gathers pre and post assessments to gauge whether the students’ knowledge has increased. The participants of the application also answer a post survey gathering the sentiment of the students after using the application.

The second case study selected was conducted by Konak (2018). The target demographic utilized by the researcher was high school students. Specifically, 10<sup>th</sup>, 11<sup>th</sup>, and 12<sup>th</sup> graders. The case study utilizes a different approach and has students attend a weeklong cybersecurity bootcamp that is

modeled from the GenCyber program. The program promotes collaboration as a key aspect of success in the program. In addition, the researcher also refers to a Self-Efficacy approach. This is defined in the research as, “An individual’s confidence in his or her ability to perform a task according to specific performance outcomes” (Konak, 2018, p.2). Thus, this research focuses on having collaboration between the students to build self-efficacy and completing the challenges utilizing a collaborative approach. Pre and post assessments were part of the program to analyze the effectiveness.

The third and final case study selected for this project was conducted by Chattopadhyay et al. (2020). This case study used a target demographic of middle-school and high school students. Given the scope of this culminating experience project, only the middle-school children’s results are utilized. This case study promotes instructor lead teaching and has the students attend various workshops based on the topics discussed. Once the workshops have been completed, the participants are taken through a game based on various privacy principles. Like the previous case studies, pre and post assessments were utilized to measure the effectiveness of the program.

### Cybersecurity Education Challenges

The final question in the culminating experience project is, “*What are unique challenges that may be encountered when implementing this type of education nationwide?*” To find the potential challenges with implementing

cybersecurity education for K-12 students the following keywords were utilized in the Google Scholar and One Search engines “Cybersecurity Education Challenges”.

The first article found using these keywords was research by Rahman et al. (2020). The research delves into the issues that affect the implementing of cybersecurity education and mentions some causes, being, “Lack of expertise, funding, and resources” (Rahman et al., 2020, p. 379). Teachers are often lacking the experience when it comes to educating students on cyberspace, this issue is magnified when schools and local governments lack the appropriate funding and resources to help better prepare educators on this topic (Rahman et al., 2020). Without access to the resources, educators and K-12 schools face a large obstacle.

The second article found utilizing these keywords was written by Triplett (2023). The researcher highlights the growing number of cybersecurity professionals around the globe due to lack of exposure to cybersecurity concepts in school. As stated in the literature, “The lack of qualified professionals to guide high school and college students on pursuing cybersecurity as a career is a significant contributor to the shortage” (Triplett, 2023, p.48). The research claims that the shortage of cybersecurity programs in high schools across the nation is going to contribute to the issue. The research also mentions the lack of funding being a root cause to the lack of security programs around K-12 schools (Triplett, 2023).

The third article was found relating to the issues in the demographics that target cybersecurity education. As stated in the research, “Educational institutions need to do more to fully embed cybersecurity practices and principles into academic programs across the educational pipeline” (Nakama et al., 2018, p.1). The researcher highlights that the minority groups and women are highly underrepresented with only about 13% of cybersecurity professionals in the United States being women and mention that women in minority groups make up a single digit percentage when it comes to representation in cybersecurity (Nakama et al., 2018). The study focuses on the challenges of providing cybersecurity education to minority groups in rural areas, specifically at the high school levels.

The final article of the literature review investigated the effect of financial deprivation on the learning outcome for K-12 aged students. Financial deprivation defined in the context of this study is, “A psychological state in which people feel financial inferior relative to a salient comparison standard because they perceive a deficit in their financial position (Prior & Renaud, 2022, p.3). Financial deprivation has many negative affects when it comes to health and has shown to affect cognitive development in young children, leading to lesser understanding essential concepts (Prior & Renaud, 2022). The research suggests financial deprivation can hinder a child’s learning of cybersecurity concepts, specifically, password best practices. When compared to peers that come from higher affluent backgrounds, children from households that suffer

from financial deprivation are less likely to retain the knowledge (Prior & Renaud, 2022). The literature that is presented in this chapter investigates the three research questions with each key word search targeting specific questions.

The goal of the research is to understand the most effective method of delivering cybersecurity education to K-12 aged individuals, identify the best practices when it comes to selecting topics suited for different age ranges, and identify unique challenges may be encountered when attempting to implement this type of education in classrooms across the United States.



## CHAPTER THREE: RESEARCH METHODOLOGY

### Selection of Research Articles

Chapter three will describe the methods and procedures that were utilized to gather the required data that will be analyzed as part of this culminating experience project. The primary case studies selected for this project were collected from scholarly search engines. The two scholarly search engines utilized for this purpose were Google Scholar and One Search. The following engines were selected due factors such as, Google Scholar allowing for the end user to broadly search for scholarly literature (About Google Scholar, n.d.) while One Search is offered through the CSU system and provides access to library content such as databases, books, and other forms of media (John M. Pfau Library, 2022). Both search engines allow for the user to fine tune the search results by setting specific search parameters. In this instance, the following parameters were utilized: English language, Open Access, and a 2010-2023 date range. Following this, specific key word searches related to the proposed research were queried into both search engines. The keywords that were selected in this process were based on their relevance to the research questions and provided results needed to support the proposed questions.

## Methodology

As described in the first chapter, the culminating experience project will seek to answer the following three questions:

1. What are effective methods to educate children and teenagers on cybersecurity concepts?
2. What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?
3. What are unique challenges that may be encountered when implementing this type of education nationwide?

The first key word search of “Effective K-12 Cybersecurity Education” focused on answering research Question 1: *What are effective methods to educate children and teenagers on cybersecurity concepts?* This holistic search provided articles that analyzed the best practices in cybersecurity education for the selected age ranges. Additionally, the studies selected in this section utilized either quantitative or qualitative data to support recommendations for specific instruction methods. A common theme found within the articles was that cybersecurity education for K-12 aged individuals is still a very new topic that requires additional research. Despite this, the articles selected during this key word search provide information and background on current cybersecurity education solutions for K-12 students. A limitation that was shared was that the articles chosen were theory based and did not include examples of the

recommendations being put into place in a real-world scenario. The lack of real-world examples influenced the following key word search.

The secondary set of key words utilized was “Cybersecurity Education Case Study”. The goal of this keyword selection was to find supporting articles for research Question 2: *What are best practices for topic selection when it comes to cybersecurity education of people in this age range?* This selection enabled the research to find practical examples of cybersecurity education for children and teenagers in elementary (ages 5-10), middle (ages 11-13), and high school (ages 14-18). A total of three case studies were selected. Each case study targeted different level of K-12 students, provided different methods of instruction, and all provided empirical data that showed student improvement. A summary of the inclusion and exclusion criteria is provided in Table 3. As stated, this secondary search will aid in answering the second research question but will also provide additional supporting evidence to the proposed teaching methods. This will be done by analyzing the outcomes of the cybersecurity bootcamp in which the students participated and investigate the methods the researchers utilized to select topics for the different age ranges mentioned.

Lastly, the search for Cybersecurity Education Challenges addresses the last research Question 3: *What are unique challenges that may be encountered when implementing this type of education nationwide?* This research will help identify unique challenges that may prevent this type of education from being implemented in the classroom. A standout reason being the lack of mentors and

opportunities for minority groups to learn about cybersecurity in school (Triplett, 2023; Nakama et al., 2018). The articles provide quantitative and qualitative research approaches to gain an understanding of the unique issues some communities may face with receiving this type of education. The information gathered will not only support the last research question but will aid in recommending further areas of study in later Chapters.

### Selection of Case Studies

The culminating experience project will utilize three case studies to investigate the process of how three K-12 schools implement a cybersecurity education program. The initial search for “Cybersecurity Education Case Study” provided numerous examples of cybersecurity education in higher education and in the workplace, but there was a lack of comprehensive literature relating to education of the targeted age groups. Therefore, the selection of the case studies utilized inclusion and exclusion criteria to make sure the selected case studies had relevancy and provide adequate information to support all three research questions that were presented in this project. The studies that were selected must have contained the following: empirical data in the form of pre and post assessment examination, showcase information related to the method of instruction and explanations as to why this instruction method was chosen, and provide an explanation of the limitations that were associated with the cybersecurity education. Additionally, the case studies must have been gathered

from a scholarly journal, written in English, and the most recent and updated version was utilized.

Table 3. Cybersecurity Education Inclusion and Exclusion Criteria

| Inclusion Criteria   | Exclusion Criteria   |
|--|--|
| The case study must be published by a reputable journal or conference proceeding.                  | Case studies published in languages other than English.                |
| The case study must contain empirical data in the form of pre and post assessment information.     | Non-scholarly literature   |
| The case study must provide information as to why the delivery method of instruction was selected. | Case studies that targeted demographics outside of the K-12 age range. |
| Describe the limitations of the study  |  |

The inclusion and exclusion criteria items were selected based on the Systematic Literature Review (SLR) process. This type of literature review “identifies, elects, and critically appraises research in order to answer a clearly formulated question” (Charles Sturt University, 2023, par. 2). This method of research was utilized in the systematic literature review conducted by Adlaon

(2023). The systematic literature review by Adlaon (2023) had an objective to answer three research questions relating to the trends, methods, and solutions of ransomware attacks in the healthcare industry. The selection criteria aided in the process as this allowed, “The selection to be more accurate based on the relevance of the targeted research questions, but also ruled out any signs of bias and other factors that may have cause the selection of certain studies to be included” (Adlaon, 2023, p.16). Figure 2. Will describe the specific criteria utilized by the researchers to select high quality articles relevant to the research questions presented.

| Criteria for Inclusion   | Criteria for Exclusion                               |
|--|--|
| The paper must be a peer-reviewed product published in a conference proceeding or journal.   | Papers written in other languages.                   |
| The paper must contain information related to ransomware, healthcare, and at least one of the following: artificial intelligence, machine learning, and blockchain technologies. | Blogs, books, and other quick read-related documents |
| The paper must present empirical data related to the topic.  |  |

Figure 2. Criteria for Healthcare Ransomware Articles (Adlaon, 2023, p.15).

## CHAPTER FOUR:

### CASE STUDY ANALYSIS AND FINDINGS

To answer the research questions proposed in this project, three case studies of cybersecurity education have been selected. The selected case studies included the three items listed in the inclusion criteria column in Table 2. In addition to the inclusion criteria, the scope of the case studies targeted different age ranges. The three age ranges in the case studies were elementary, middle, and high school aged students. This age range was selected as it is theorized that the teaching styles utilized for a 1<sup>st</sup> grade student may be drastically different from a 12<sup>th</sup> grade student. According to Jean Piaget's theory of Cognitive Development, a child goes through four stages of thinking from infancy to adolescence (Joubish & Khurram, 2011). The four stages are summarized in Table 4 below.

Table 4. Summary of Jean Piaget's Theory of Cognitive Development (Joubish & Khurram, 2011, p. 1262)

| Stage Of Development          | Characteristic of Stage  |
|-------------------------------|--|
| Sensori-motor (0-2 years old) | Differentiates self from objects, recognizes self as an agent of action, |

|   |   |
|---|---|
|   | and acts intentionally, achieves object permanence  |
| Pre-Operational (2-7 years old)             | Learns to use language and to represent objects by images and words.<br>Egocentric style of thinking.<br>Classification of objects.                                       |
| Concrete Operational (7-11 years old)       | Able to think logically about objects and events. Classifies objects according to several features.   |
| Formal Operational (11 years old and above) | Ability to think logically about abstract propositions and test hypotheses systematically. Becomes concerned with the hypothetical, the future, and ideological problems. |

The broad age range was selected due to the lack of related case studies for specific age groups. As cyber security becomes a growing topic of concern due to growing numbers of cyberattacks across the globe, the lack of case studies of this type of education may be a temporary issue. Considering this, the following section will be an executive summary of each case study and how each case study addresses the three proposed research questions found in Chapter 1.



## Case 1: Cyber Aware

Cyber Aware is a gamified learning platform designed to introduce elementary school aged children to basic concepts of cybersecurity and privacy. The usage of a digital game-based learning (DGBL) platform was chosen by the researchers due to electronic devices establishing themselves in learning environments and students often finding such platforms, “More attractive and personalized” (Giannakas et al., 2019, p. 82). In addition to this, the researcher further states that, “Given that the great majority of children and teenagers experience the internet via mobile devices, the positive outcomes of DGBL can be further enhanced if the learning content is delivered via the use of a mobile app” (Giannakas et al., 2019, p. 82). As the number of persons in the elementary school age range that are exposed to technology increases, the research explains the growing need for similar platforms.

**Question 2:** *What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?*

To construct the security and privacy curriculum within the platform, the researchers utilized a variety of cybersecurity educational materials from around the world. This is due to the lack of standardization related to cybersecurity education, which is a sentiment shared with the research article by Domeji (2019)

referenced in earlier chapters. A list of the documentation utilized to support the curriculum is detailed below:

1. CERIAS K-5 Information Security Curriculum (Kindergarten – 5<sup>th</sup> Grade)
2. Australian Government eSafety Classroom Resources (Preschool – 7<sup>th</sup> Grade)
3. UK Government GetSafeOnline resources (6 – 9 Years of Age)
4. The National Cybersecurity Alliance StaySafeOnline Resources (3<sup>rd</sup> – 5<sup>th</sup> Grade)
5. The National Integrated Cyber Education Research Center Cyber Literacy curriculum (K-12)

Giannakas et al. (2019) suggested that the above content guidelines target children from 6-12 years old and were part of notable cybersecurity campaigns with the goal to:

Familiarize learners with fundamental cybersecurity technologies that are required to keep their Internet-connected devices protected against legacy threats, as well as to keep their passwords safe. Second, it aims at raising learners' awareness on privacy issues mostly related to their identity and the protection of their personal information published on the web. (p. 85)

Once curriculum was created utilizing the above information. The researchers following objective to find a suitable model of education for the scoped age range of the application.

Question 1: *What are effective methods to educate children and teenagers on cybersecurity concepts?*

To deliver the information in the above documentation in an educational format Giannakas et al. (2019) utilized the Attention, Relevance, Confidence, and Satisfaction (ARCS) model of motivation. The main goal of this model is to, “Spur motivation by systematically guiding the design of engaging learning activities that produce specific learning outcomes according to the learner’s behavior” (Giannakas et al., 2019, p. 92). The four mentioned categories of Attention, Relevance, Confidence, and Satisfaction are broken up into multiple subcategories. Each one of the subcategories listed is tied to specific items found within the Cyber Aware application. These are presented in the activities, notifications, and assistance popups. A breakdown of how the researchers designed the learning content of the platform can be found in Figure 3 below. A breakdown of core concepts of the ARCS model will be detailed in the following sections.

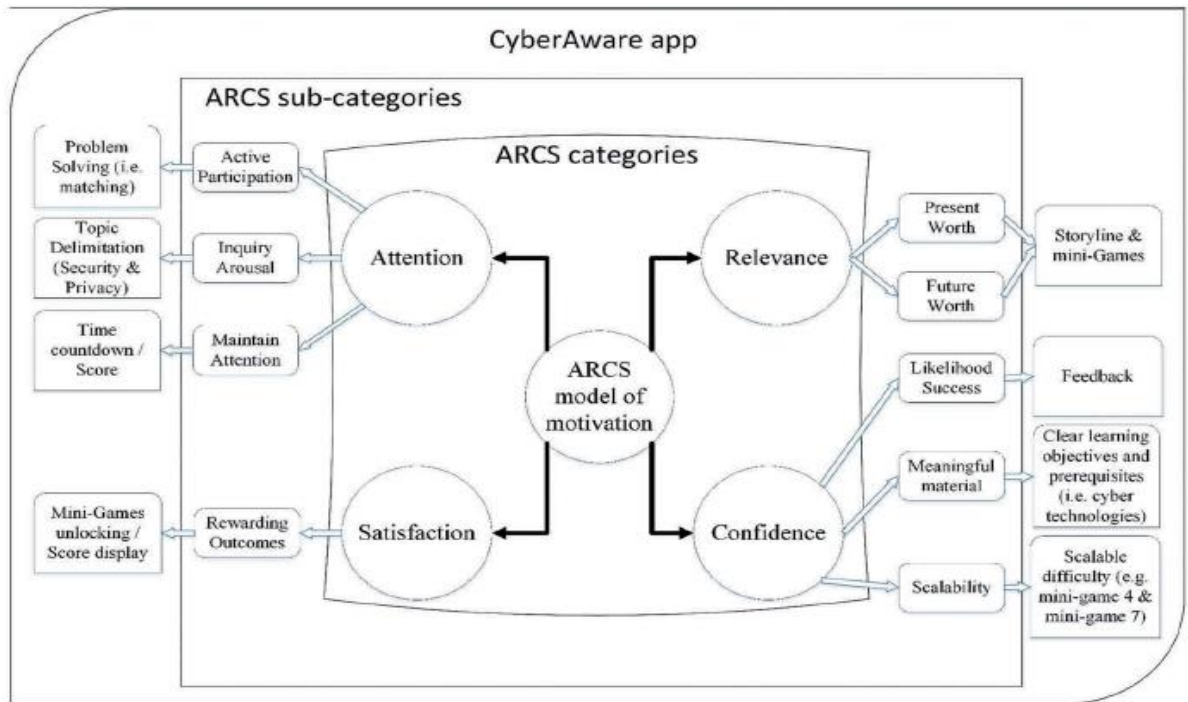


Figure 3. Cyber Aware ARCS Categories (Giannakas et al., 2019, p. 93)

### Attention

Attention is the first goal found in the ARCS model of motivation. The researchers Giannakas et al. (2019) find this to be one of the critical steps in this model as keeping students engaged at a high level would correlate to positive learning outcomes. The way this research fulfills the attention component of this model is through active participation, inquiry arousal, and maintaining attention. These three subcategories are addressed in multiple sections throughout the game platform.

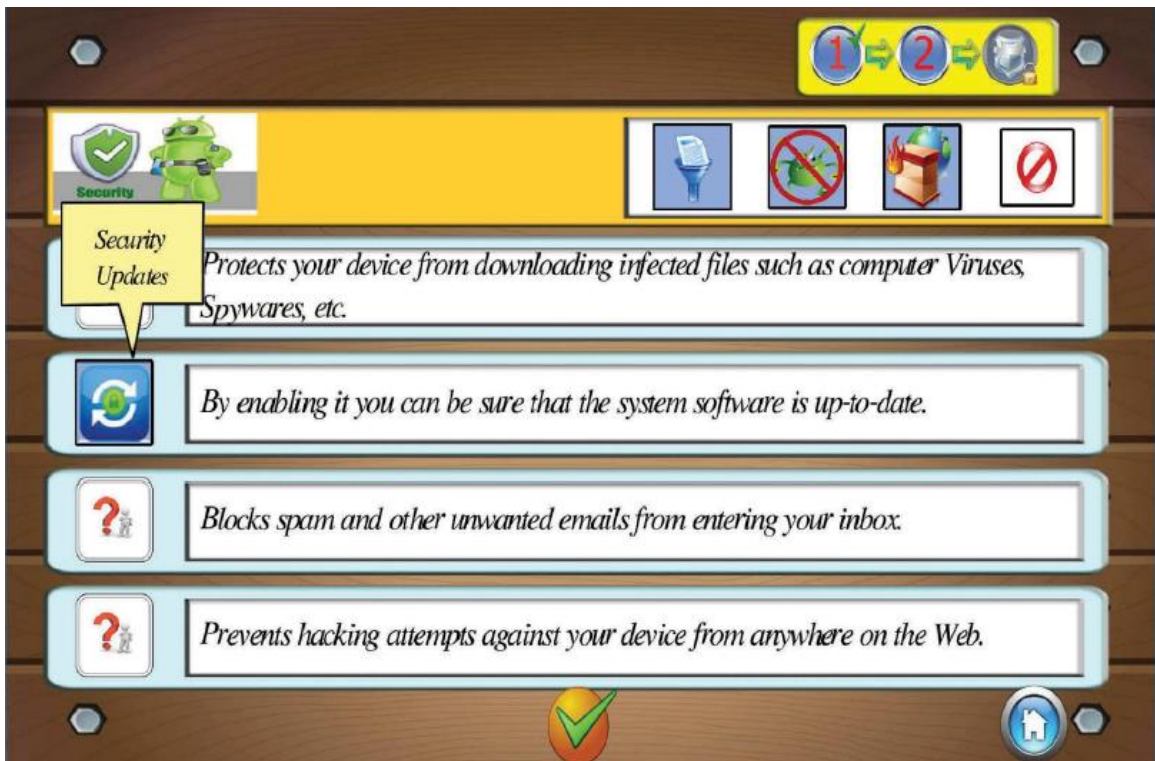


Figure 4: Mandatory Security Module (Giannakas et al., 2019, p 87).

The researchers claim that the students are actively participating in the game modules as they must mandatorily play through the games to advance to the following sections (Giannakas et al., 2019). An example of one of the mandatory sections can be found within Figure 4.

### Relevance

The Relevance component of the ARCS model focuses on keeping the retention of the learner's interest in the topic that is being presented. The researchers present ways of this being accomplished: "Providing merit of the course and its goals, and (b) its relevance to real-life problems and situations"

(Giannakas et al., 2019, p. 93). The method of this being completed through the Cyber Aware platform is using a storyline that shows the importance of the task that is being presented to the students and the importance of said task. An example of this is presented in Figure 5.



Figure 5. Relevance of Task Introduction (Giannakas et al., 2019, p.94)

### Confidence

Confidence is the third component in the ARCS model of motivation. The goal of this component is to allow the students to feel a sense of accomplishment when completing a task to avoid falling out of the learning process (Giannakas et al., 2019). For students to feel accomplished, they cannot be given tasks that are

too difficult nor too easy as each end of the spectrum may cause the students to become overwhelmed or overconfident. If a student becomes overwhelmed, the feeling of self-doubt may become a factor leading to poor learning. On the other hand, if the given tasks are too easy, the students will not be motivated to try and once they are challenged, they may begin to feel discouraged. The Cyber Aware platform addresses the confidence component by gradually increasing the difficulty of the tasks as the user progresses through the platform.

### Satisfaction

The final component in the ARCS model of motivation is Satisfaction. This component addresses the feelings that the students receive while completing the modules and after the platform has been completed. If the students feel positive during and after the program, the likelihood of them retaining the information is higher. This was accomplished through visual advancement and a scoring system visible to the students. The visual advancement shown within the application is visible in Figure 6. By unlocking different levels within the game to eventually unlock the shield. An example of the scoring system is provided in Figure 7. By the students advancing through the module and answering questions correctly, they are rewarded with a higher score which is always visible.



Figure 6: Visual Advancement (Giannakas et al., 2019, p.90)

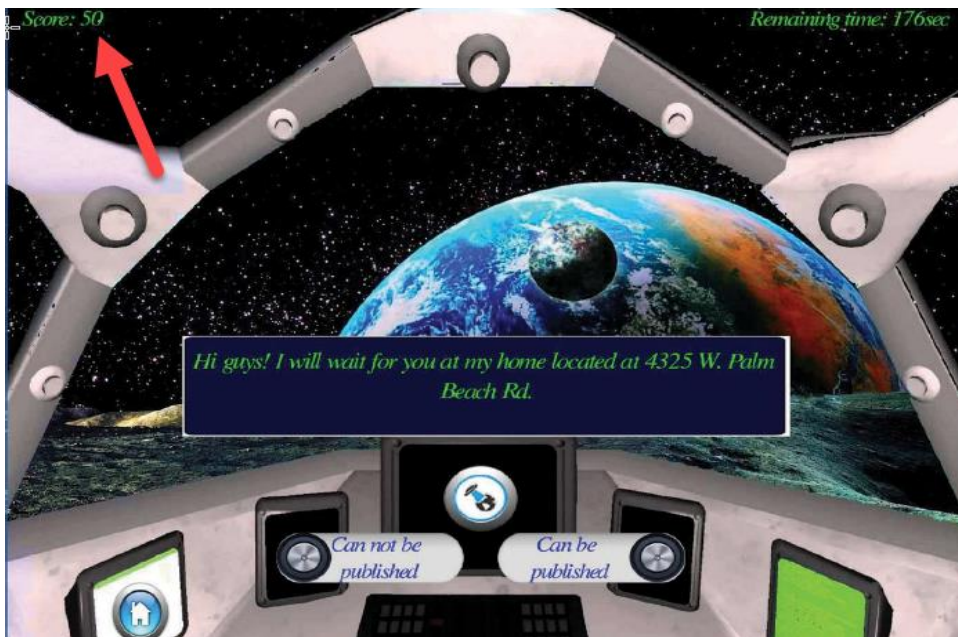


Figure 7: Scoring System (Giannakas et al., 2019, p.90)



To understand the effectiveness of the Cyber Aware platform. The research utilized a control group of 26 participants and a treatment group of 26 participants. Both the control and treatment groups were given two 45-minute lectures throughout a week utilizing traditional instructor led education. After this week, a Pre-Test was distributed to the students to gauge their knowledge of cybersecurity and privacy fundamentals. After the Pre-Test was administered, the control group was provided access to the Cyber Aware platform for two 45-minute sessions while the control group received an additional two 45-minute sessions of instructor led education. At the end of this following week, both control and treatment group participated in a post-test. A summary of the results can be found in Figure 8.

| Description   | Before playing the game | After playing the game |
|---|-------------------------|------------------------|
| Learners recognized all 4 technologies that are required to keep their Internet-connected devices protected         | 34.6%                   | 53.8%                  |
| Learners recognized more than 3 learning scenarios out of 6 that an Internet-connected device needs to be protected | 34.6%                   | 65.4%                  |
| Learners recognized all the learning scenarios that an Internet-connected device needs to be protected              | 7.7%                    | 38.5%                  |
| Learners recognized all the desirable qualities of a strong password  | 26.9%                   | 42.3%                  |
| Learners identified the wrong formatted password  | 19.2%                   | 65.4%                  |

Figure 8. Summary of Cyber Aware Results (Giannakas et al., 2019, p. 99)

**Question 3:** *What are unique challenges that may be encountered when implementing this type of education nationwide?*

The final question relating to the unique challenges that may arise is the mass implementation of platforms like the Cyber Aware application. The researcher states that the application is installed locally on the machines within the school and utilizes minimal resources on a computer when installed and open. The problems that arise with implementing an application on each machine locally are the potential vulnerabilities of the application as it needs to be internet facing is the instructors would like to use any of the Learning Management System (LMS) functionality to track students' progression. In addition to this, some schools may not have adequate resources to support such installations. Rural schools and school districts in lower income school districts may have limited technological resources or instructors with adequate skills to support such education (Nakama et al., 2018).

#### Case 2: Penn State Berks

The second case study selected is from the University of Penn State Berks. The purpose of this case study is to review the effectiveness of a weeklong in person cybersecurity bootcamp for 10<sup>th</sup>, 11<sup>th</sup>, and 12<sup>th</sup> grade students. The cybersecurity bootcamp hosted by the university was part of the GenCyber cybersecurity outreach program. The goal of the GenCyber program

created by the National Security Agency (NSA) is to, “inspire the next generations of cyber stars by working with academia and federal partners to ignite cybersecurity awareness, increase interest, and teach sound cybersecurity fundamentals that strengthen the cybersecurity education ecosystem and the Nation’s future workforce” (GenCyber, 2023). Therefore, the GenCyber movement hopes to close the current gap of knowledge in cybersecurity for K-12 students.

*Question 2: What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?*

The case study from Penn State Berks encompasses high school students from 10<sup>th</sup>, 11<sup>th</sup>, and 12<sup>th</sup> grade. To achieve adequate learning of cybersecurity concepts, the requirements set forth by the NSA for these bootcamps is to introduce cybersecurity first principles through, “activities that involve problem-solving, decision making, reasoning, critical thinking, and creating” (Konak, 2019, p. 1). Although the GenCyber programs require these principles to be instilled, there is not a curriculum guideline provided by the NSA for participants of the program. Therefore, the individuals leading the GenCyber camps are responsible for developing the curriculum and deciding the instructional methods that will be utilized (Konak, 2018). In this instance, the researcher created a weeklong curriculum based on common tasks that a cybersecurity professional may

encounter as part of their work duties. As the work of a cybersecurity professional may be broad, this approach attempts to encompass every facet ranging from systems administration, networking, and policies to peak the participants interest in cybersecurity as a career path. A sample of the weeklong curriculum that is utilized by Pen State berks is found in Figure 9 below.

| Lecture Topics  | Sample Learning Objectives  | Hands-on Activities  |
|---|---|--|
| <b>Day 1:</b><br>Data Encoding and Decoding<br>Introduction to TCP/IP   | <ul style="list-style-type: none"> <li>-Describe TCP/IP addressing &amp; port numbers</li> <li>-Use basic networking commands in Windows</li> <li>-Describe port numbers</li> <li>-Explain client/server paradigm</li> <li>-Create backdoors to exploit network applications</li> </ul>   | <ul style="list-style-type: none"> <li>-Number systems</li> <li>-Data encoding and decoding</li> <li>-CVCLAB Login Tutorial</li> <li>-Introduction to Networking with Windows 7 (TCP/IP Lab)</li> <li>-Netstat &amp; File Sharing</li> <li>-Netcat</li> </ul>  |
| <b>Day 2:</b><br>TCP/IP Protocol<br>Malware, Trojans, Viruses,<br>Social Engineering Attacks<br>Introduction to Linux Kali<br>Network Attacks | <ul style="list-style-type: none"> <li>-Describe the functions of the TCP/IP protocol layers</li> <li>-Use a packet analyzer to analyze network traffic</li> <li>-Classify various types of malware</li> <li>-Use standard techniques to identify malicious activity on a computer</li> <li>-Explain how social engineering can be used to gain access to systems</li> <li>-Define the threats posed to networks</li> <li>-Discuss methods to defense against network attacks</li> </ul>                      | <ul style="list-style-type: none"> <li>-Analyzing IP packets in Wireshark</li> <li>-Creating a Trojan Horse</li> <li>-Keylogger</li> <li>-Phishing IQ Test</li> <li>-Linux networking tools</li> <li>-IP Spoofing</li> <li>-Denial of Service Attacks</li> <li>-Hacking Using Armitage &amp; the Metasploit Framework</li> </ul>   |
| <b>Day 3:</b><br>Data Confidentially<br>Traditional Ciphers<br>Attacks on traditional ciphers<br>Symmetric Algorithms<br>Key exchange         | <ul style="list-style-type: none"> <li>-Describe data confidentiality</li> <li>-Describe the process of encryption/decryption</li> <li>-Explain cipher operators</li> <li>-Conceptualize the strength of a cipher</li> <li>-Describe the strength of an encryption algorithm (diffusion versus confusion)</li> <li>-Describe components of block ciphers</li> <li>-Apply symmetric algorithms for confidentiality</li> <li>-Test cryptographic strength of ciphers</li> <li>-Describe key exchange</li> </ul> | <ul style="list-style-type: none"> <li>-Stick Cipher, Caesar Cipher &amp; Scytale Cipher in Cryptool</li> <li>-Brute force attacks</li> <li>-Frequency analysis</li> <li>- Mini project: design your traditional cipher</li> <li>-Data encoding/decoding in Cryptool</li> <li>-Using Symmetric Algorithms (AES)</li> <li>-Comparing RC4 and AES</li> <li>- Impossible: Mission Game</li> </ul> |
| <b>Day 4:</b><br>Data Integrity<br>Password Attacks<br>Steganography<br>Digital Forensics   | <ul style="list-style-type: none"> <li>-Apply data integrity methods to verify files and messages</li> <li>-Describe various methods to attack passwords</li> <li>-Explain the need for strong passwords</li> <li>-Describe the process of a digital investigation</li> <li>-Explain the tools and techniques used in a digital investigation</li> <li>-Use file carving techniques to recover digital evidence</li> </ul>  | <ul style="list-style-type: none"> <li>-Hash functions</li> <li>-Password cracking</li> <li>-Using jphide and jpseek</li> <li>-Rhino Digital Forensic Case</li> </ul>  |
| <b>Day 5:</b><br>System Hardening<br>Penetration Testing  | <ul style="list-style-type: none"> <li>-Explain the roles of policies</li> <li>-Apply policies to secure computer systems</li> <li>-Describe the penetration testing process</li> <li>-Apply penetration testing tools to scan networks and hosts</li> <li>-Use penetration testing tools appropriate to the task</li> </ul>  | <ul style="list-style-type: none"> <li>-Firewalls</li> <li>-Local Security Policies</li> <li>-Group Policy</li> <li>-Target discovery</li> <li>-Target enumeration</li> <li>-Vulnerability assessment</li> </ul>   |

Figure 9. Weeklong GenCyber Bootcamp Curriculum (Konak, 2018)

**Question 1:** *What are effective methods to educate children and teenagers on cybersecurity concepts?*

The curriculum designed by the hosts of the GenCyber program at Pen State Berks aimed to introduce students to different domains that cybersecurity professionals may encounter. The method of introducing cybersecurity instruction to students is vital to successful learning (Konak, 2018). It is found that many researchers recommend hands on learning as an efficient method of teaching strategy for K-12 age range (Konak, 2018; Giannakas et al. 2018; Javidi & Sheybani, 2019; Domeji, 2019). While the case study is supportive of this teaching style, it is expressed that not all hands-on learning activities provide the same quality of education, as some students may blindly follow on screen instructions without fully understanding the concepts. (Konak, 2018). Therefore, the case study attempts to present a method of delivering security education by promoting collaborative and hands on learning between the participants of the GenCyber camp.

To promote a collaborative environment, the GenCyber camp utilizes a hands-on inquiry-based approach. The researcher outlines this approach as such, “Each hands-on activity includes four components: concrete experience, reflective observation, abstract conceptualization, and active experimentation” (Konak, 2018, p. 6). A brief description of the 4 components is described in Table

3. In addition to this, an example of how the four components is integrated into the students' learning activities is found in Figure 9.

The effectiveness of the program was measured in pre, and post assessment surveys provided to the participants on the weeklong camp. From the results, the students were able to drastically improve their knowledge in the domains covered by the course curriculum. For example, in the domain of Systems Administration, there was a 42% increase in the post assessment surveys. The in the following domain of Networking, the students saw an increase of 63% after the bootcamp. The researcher attributes the drastic improvements to hands on inquiry-based approach. As stated by Konak (2018), "The active reflection and abstract conceptualization components of the activities encouraged the participants to construct knowledge rather than memorize it" (p. 9). This type of learning followed by encouraging the students to reach out to each other for assistance when issues were faced during the activities allowed for the students to identify their gaps in learning and sought to gather the information via their peers (Konak, 2018).

Table 5. Program Component Description

| Component                  | Description  |
|----------------------------|--|
| Concrete Experience        | Step-by-step instructions are provided to students to guide them through the activities. This may include the usage of visual aids. Instruction is given until students reach a satisfactory level of knowledge. |
| Reflective Observation     | Conducted after the concrete experiences through means of discussions and reflections on the activities. High levels of student interactions were in place to enhance the reflection.                            |
| Abstract Conceptualization | Concept supported by the instructor of the program. Students are asked questions related to the activity to gauge understanding. Usage of generalized questions surrounding the covered topics.                  |
| Active Experimentation     | Completion of tasks with little or no guidance. Encouragement of students to work together to recall the instructions, the previous tasks to complete the new challenges presented.                              |

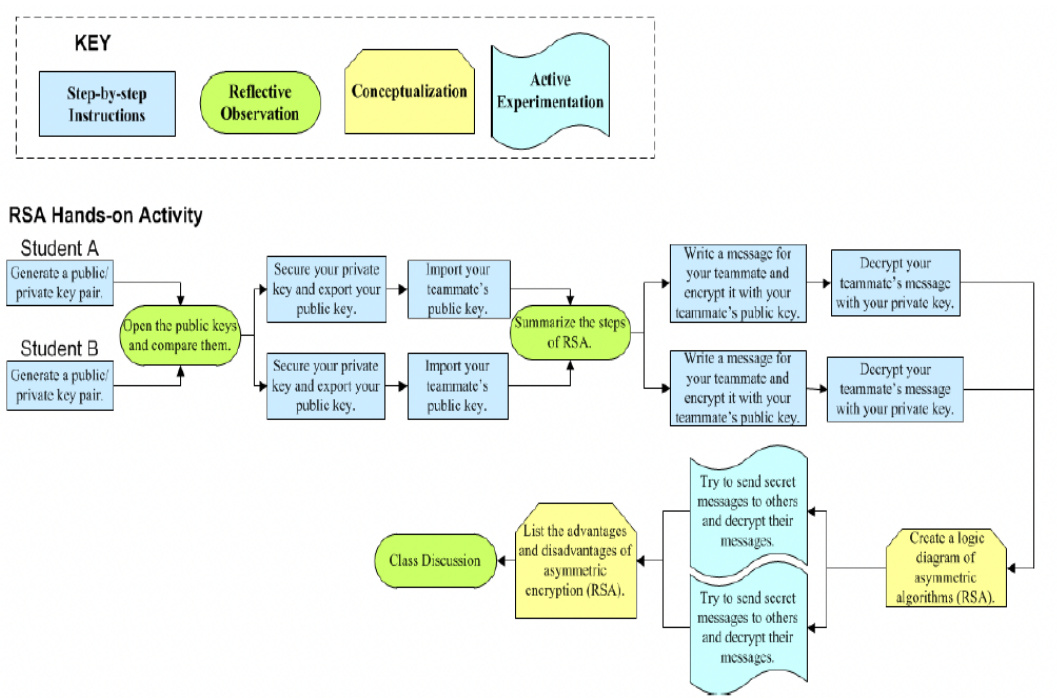


Figure 10. Program Component in Hands-on Activity (Konak, 2018, p.7)



Question 3: *What are unique challenges that may be encountered when implementing this type of education nationwide?*

The unique challenges that may arise from implementing this type of program across the nation would be the lack of standardized curriculum available for the GenCyber programs. As previously mentioned, the hosts of the camps are instructed to deliver the cybersecurity-first principles but are not provided guidance as to what the specific curriculum requires (Konak, 2018). This may prove to be challenging for schools that lack the resources to have full time cybersecurity subject matter experts on staff as cybersecurity lessons are typically taught by an expert in the field (Domeji, 2019). The construction of the curriculum will also be dependent on the cybersecurity subject matter experts as the domain of cybersecurity is very broad the concepts within the domain may be found to be described as a “Very dry topic for K-12 students” (Konak, 2018). Therefore, collaboration between experts in cybersecurity and education will need to collaborate to create an effective plan for students at all age levels in K-12.

In addition to this, the GenCyber program is limited in funding and resources. In 2023, there were a total of 150 camps in 44 states (GenCyber, 2023). While the programs were able to reach out to a total of 3300 students and 800 teachers at the time of this case study, the cybersecurity outreach done by these programs are still found to be in the infancy stages. Many schools found in minority or rural communities do not have the resources in terms of cybersecurity

personell or universities with the ability to host a GenCyber or similar styled cybsecurity bootcamp (Nakama et al., 2018).

### Case 3: Visual Privacy Learning Tool

The following case study by Chattopadhyay et al. 2020 focuses on educating middle and high school students on the topic of Privacy in Cybersecurity. The focus on privacy comes from the General Data Protection Regulation (GDPR) rules affecting technology and business operations globally as, “Consumer privacy has now become far more significant and relevant for email, internet, and other information technology service users” (Chattopadhyay et al. 2020, p.2). Specifically, the visual-privacy domain has currently been found to be the most underestimated and under prepared topic in the scope of information security practices (Chattopadhyay et al., 2020). Chattopadhyay et al. (2020) suggested the use of a novel visual-privacy themed game-based learning platform to educate K-12 students covering, “societal-security and human-privacy topics, ethics and trust notions, as well as expose them to basic information-security concepts in a simple, entertaining yet engaging hands-on tool-oriented lesson plan” (Chattopadhyay et al., 2020, p.2). A sample of the learning tool interface is pictured in Figure 11.



Figure 11. Sample of Visual Privacy Application Interface (Chattopadhyay et al.2020, p.4)

The study conducted by Chattopadhyay et al. (2020) had both middle and high school students within the scope. Since the high school age range was discussed in the previous case study, only the numbers from the middle school participants will be considered for the purposes of this Culminating Experience Project.

Question 1: *What are effective methods to educate children and teenagers on cybersecurity concepts?*

The advent of digital device usage by adolescents has increased drastically and privacy is becoming an area of concern with these applications. As people in this age range lack an understanding of how privacy works in these public domains, they are highly susceptible to compromising their privacy and confidentiality of personal information (Chattopadhyay et al., 2020). For the purposes of effectively educating middle school students in cybersecurity and privacy concepts, Chattopadhyay et al. (2020) utilized a computer-based visual learning tool in their case study. The researchers reasoned that the tool created for the purpose of the case study is a novel tool and the only one available at the time of publishing. The reasoning behind the creation of the visual learning tool is, "Existing literature shows that multimedia-based teaching of privacy concepts is effective and makes a difference" (Chattopadhyay et al., 2020, p.2). As the visual-privacy experimental learning tool falls into the category of multimedia-based learning the researcher hypothesized that the tool would prove to show significant learning outcomes for the participants.

The learning plan is structured with topics that will relate to real world scenarios the students may encounter while being online. The secondary goal of the learning tool is to be entertaining to help keep the students interested throughout the workshop. Engaging students in curriculum they can relate and find interesting has been proven to be a successful method of delivering cybersecurity instruction as this was seen in the previous case study conducted by Konak (2018). Therefore, the researcher aims to, "Spark the young minds and

encourage them to further explore computing security and privacy related topics” (Chattopadhyay et al., 2020, p.4).

Question 2: *What are best practices for topic selection when it comes to cybersecurity education of people in the 3-18 years age range?*

For the purposes of designing the curriculum for the visual-privacy tool, the researcher designed the curriculum around numerous topics in the Information Technology (IT) and Cybersecurity domains. The following topics are found to be part of the curriculum, “Basic computing and IT knowledge elements, e.g., human-privacy, societal-security, trust, privacy versus security tradeoffs, public surveillance related concepts, and ethics” (Chattopadhyay et al., 2020, p.4). As the topics encompass the IT and Cybersecurity domains, the researchers formulated the curriculum to also consider the concept areas under the Computer Science Teachers Association (CSTA) K-12 Computer Science Standards such as: computational thinking, collaboration, safety, law, and ethics. In addition to this, the researchers also utilized the Security-First principles that are part of the GenCyber program. A mapping of the GenCyber cybersecurity first principles and the curriculum mapping for the case study will be found Figure 12.

| <b>GenCyber Security Principles and Concepts</b>   | <b>Mapping Justification/Relevance</b>  |
|--|---|
| Data/Information Hiding, Layering (Principles); Confidentiality, Integrity, Defense, Adversarial Thinking (Concepts) | Privacy Protection, Cryptography, Use of Cryptographic Obscuration (PICO)                                 |
| Least Privilege (Principle); Availability, Integrity, Defense (Concepts)   | Privacy Controls, Profile and Face Recognition Driven Visual-Privacy, Restricted Access to Image Contents |
| Minimization (Principle); Confidentiality, Availability, Defense (Concepts)  | Minimization of Image Content Visibility  |
| Simplicity (Principle); Keep It Simple (Concept)   | Use of Identity Obscuration Through Simple Face Recognition   |
| Abstraction (Principle)  | Simplified Simulation of An Enhanced Video-Surveillance Model   |

Figure 12. GenCyber Principles & Concepts Map: Visual-Privacy Learning Model (Chattopadhyay et al., 2020, p.5)

Once the curriculum was formulated, the researchers conducted two workshops that engaged middle school students with the visual-privacy tool. The total number of middle school participants of the workshops was 53 total students between the ages of 11 and 13 years old. The researcher also noted that the students came from a diverse group of underrepresented populations from public school districts near the workshop. The workshops were single sessions of 1 to 1.5 hours in length and conducted on computer workstations that were provided to the students during the workshop. Before participating in the workshop, the students were encouraged to take an anonymized pre-assessment survey which

gauged the student's interest and knowledge of cybersecurity and privacy concepts. Following the pre-assessment, the students were provided instruction on how to utilize the tool and were also provided time to work through the application. Once completed, the students participated in an anonymized post assessment survey. This concluded the workshop, and the results were analyzed by the researchers.

A survey was used to assess the effectiveness of the program. Figure 13. will provide a visual representation of the student's interest rates of computer science and cybersecurity before and after participating in the workshop.

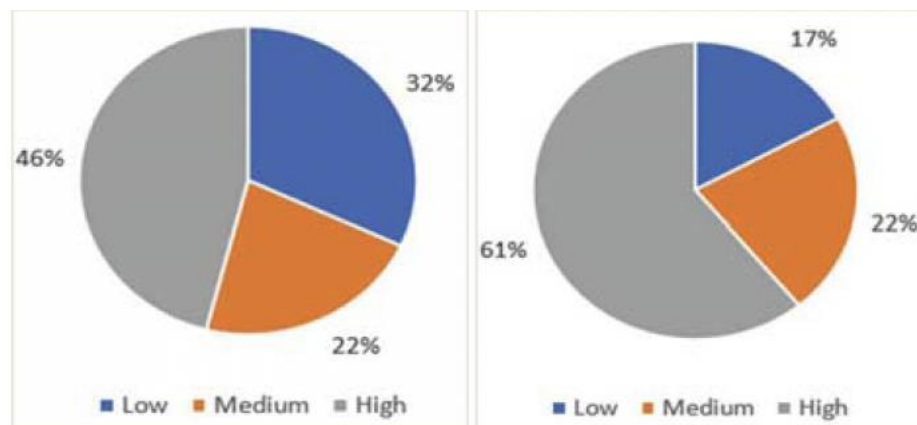


Figure 13. Student Interest in Computer Science and Cybersecurity (Chattopadhyay et al., 2020, p.6)

From the above image, it is visible that many students showed an increase in cybersecurity and computer science concepts. A 15% increase in High interest is

seen after participating in the workshop. The workshop also helped expose students to many topics which they have not experienced previously. To gauge the knowledge acquired during the program, the participants held collaborative surveys utilizing the Kahoot platform. A sample of this is provided in Figure 14 below. While the researcher did not have quantitative numbers to describe the improvements of students' knowledge of the topics, the researcher claims that the students experience higher levels of learning and interest in cybersecurity and privacy concepts.

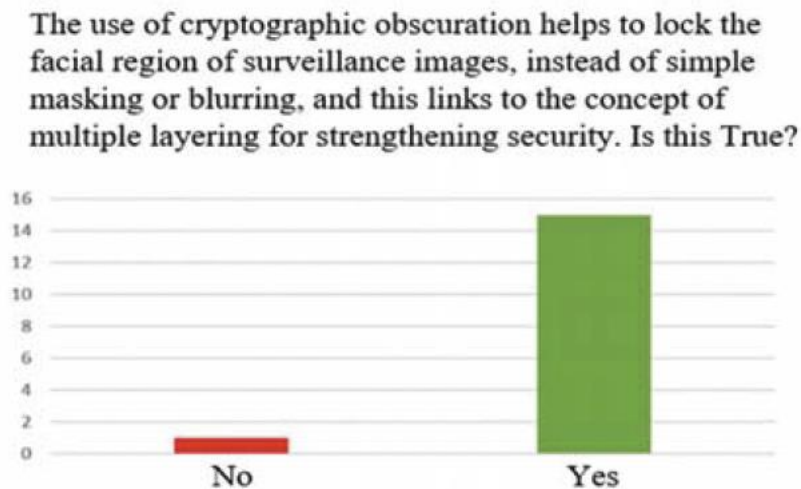


Figure 14. Sample Question and Participant Response (Chattopadhyay et al., 2020, p.8)

Question 3: What are unique challenges that may be encountered when implementing this type of education nationwide?



Unique challenges that may arise from implementing this sort of workshop nationwide are the application that was developed is the first in its class. The topic of visual privacy is, “the weakest link of data-security practices, as well as the most underestimated and underrated topic under the data-privacy domain” (Chattopadhyay et al., 2020, p.1). Therefore, there are not many case studies that can support the idea that such an application can be implemented in a large-scale setting. Like the CyberAware platform, this application is installed locally on a computer and may prove to be challenging to gain approval of school system administrators as the application may introduce vulnerabilities into the school systems.

A shared sentiment between the case studies that have been reviewed is that they rely heavily on cybersecurity subject matter experts to deliver the instruction. This is a problem as a leading cause of the shortage of interest in security is the lack of mentorship opportunities for students due to the small number of cybersecurity professionals currently (Triplett, 2023, p.48). In addition to this, the lack of resources and availability of such programs for schools in underrepresented and lower income school districts creates a large hurdle for many students across the United States.

CHAPTER FIVE:  
DISCUSSION, CONCLUSION, AND RECOMMENDATIONS FOR FUTURE  
RESEARCH

Chapter five is the concluding chapter of the project and will discuss the findings from Chapter 4, provide a conclusion on the information that was gathered, and provide potential areas of further study for each of the questions that were proposed.

Question 1: What Are Effective Methods to Educate Children and Teenagers on  
Cybersecurity Concepts?

Question 1 focused on identifying effective methods of delivering cybersecurity education for children and teenagers within the 3-18 age range. From analysis of the case studies, it was found that not only did the students substantially increase their knowledge of cybersecurity concepts in post examination surveys, but it was also found that student interest in the field of cybersecurity also increased. Additionally, it was found that these workshops were some students' first time being exposed to cybersecurity concepts. Therefore, hands on in person workshops with the goal of educating children and teenagers in these concepts were shown to be very effective by utilizing hands on and game-based learning. These types of in person workshops also provide a

first-time learning environment for many students as cybersecurity resources are scarce and provided in non-organized sporadic methods (Domeji, 2019).

An area of further study that will follow this question would be to conduct a workshop utilizing a remote learning model. The bootcamps and workshops reviewed as part of this project all take place on campus within a university environment. This type of learning environment may not be available to students located in more rural school districts that may not have the appropriate resources or personnel to host these types of sessions (Nakama et al., 2018). By analyzing the learning of an online learning environment this may open further discussions to bring security education to a larger audience across the United States.

Question 2: What Are Best Practices for Topic Selection When It Comes to Cybersecurity Education of People in the 3-18 Years Age Range?

Question 2 was answered by the three case studies via evaluating the resources that were utilized to formulate the curriculum for the bootcamps and workshops. All three of the case studies utilized information that was publicly available and published by government bodies or government sponsored agencies. It was found that the researchers utilized age-appropriate education materials for each level. As seen in the CyberAware case study by Giannakas et al. (2019), materials such as the CERIAS K-5 Information security curriculum and the Australian Government eSafety Classroom Resources were created for Preschool through 5<sup>th</sup> grade learners. While the Cyber First principles in the

GenCyber program discussed in the case studies by Konak (2018) and Chattopadhyay et al. (2020) are more catered towards the middle and high school age level (6<sup>th</sup>-12<sup>th</sup> Grade).

The best practice documents utilized in the case studies provided a good baseline of information regarding cybersecurity education, but it was found that there is not an outlined best practice guidance for how to implement such education in the classroom. Although the documents were crafted for specific age groups, these were purely recommendations set forth by the publishers and found to be items that the educators must seek out and are not readily available (Giannakas et al., 2019; Domeji, 2019; Rahman et al., 2020). As cybersecurity education becomes a growing concern, an area of future research may be to evaluate a curriculum for the age ranges listed. As theorized in Piaget's Theory of Cognitive Development, learning styles differ between children as they progress in age, therefore, narrowing the scope to focus on a specific educational group (e.g., Elementary school, Middle school, High school students) may provide further insight to how receptive the students are to cybersecurity education.

Question 3: What Are Unique Challenges That May Be Encountered When Implementing This Type of Education Nationwide?

Question 3 examined the factors that may arise from implementing cybersecurity education nationwide. The case studies provided different methods

of delivering the instruction to the students but also highlighted issues that may come with their individual implementation.

The first case study by Giannakas et al. (2019), proposed a game-based learning platform that is installed locally on a computer that has a web-based learning management system (LMS) embedded to track the students' progress. The issue highlighted in this case study is the need for the application to be installed on machines locally within the K-12 school environment, in addition to this, the web-based learning management system is critical to track the students learning progress. As the application was designed for a small case study of elementary school students, the application may have unknown vulnerabilities that have not been considered. This sentiment is shared with the case study conducted by Chattopadhyay et al. (2020) as this application is also an on-premises installation on school computers. The implementation of on premises applications in the school network may require resources such as funding for computers and staff that are not available for schools in lower income and rural school districts (Nakama et al., 2018; Prior & Renaud, 2022). Lastly, the GenCyber case study conducted by Konak (2018) highlighted an issue of availability of similar programs around the country. As of 2023, it was reported that there was a total of 150 GenCyber camps around 44 states with an outreach of 3300 students (GenCyber, 2023). According to the National Center for Education Statistics (2021), a total of 49.3 million students were enrolled in K-12 schools, when compared to the number of students exposed to the GenCyber

program, this number is only 0.0066% of students enrolled in schools in the United States. Effective outreach and increased funding is needed to bring this type of program to more schools and students around the country. Further areas of study would be to researching the creation of an online learning model that will allow for greater reach to students across the nation.

### Conclusion

In conclusion, the culminating experience project reviewed three case studies with the goal of educating K-12 students in cybersecurity concepts. The case studies provided answers to the three proposed research questions and discovered further areas of future research. It was determined from the case studies that the students experienced high levels of interest and learning outcomes after participating in the cybersecurity bootcamps and workshops. The method of selecting topics varies by age level and researchers utilized public documentation available from government and government sponsored entities, but no official guideline for teachers to follow. Lastly, the limitations that come from attempting to implement this education at a large scale come from budgetary constraints that face many schools and the lack of cybersecurity awareness outreach program at the federal, state, or local district levels.

## REFERENCES

- Adlaon, J. K. (2023). *A Systematic Literature Review of Ransomware Attacks in Healthcare* (Publication No. 1659). [Master's thesis, California State University San Bernardino]. Scholarworks.
- Ahmad, N., Laplante, P. A., Kassab, M., & DeFranco, J. (2021). A Cybersecurity Educated Community. *IEEE Transactions on Emerging Topics in Computing*, 10(3), 1456–1463. <https://doi.org/10.1109/tetc.2021.3093444>
- Ayeyemi, M. (2023). *A Systematic Review of Cybersecurity Education in K-12 Context* (Publication No. 21472). [Master's thesis, University of Eastern Finland]. Itä-Suomen yliopisto.
- Bullée, J., Montoya, L., Pieters, W., & Junger, M. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, 11(1), 97–115. <https://doi.org/10.1007/s11292-014-9222-7>
- Chattopadhyay, A., Christian, D. R., Oeder, A., & Budul, I. (2020). A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy & Societal-Security Awareness in Middle-School and High-School Youth. *IEEE Frontiers in Education Conference*. <https://doi.org/10.1109/fie43999.2019.9028375>

Criollo-C, S., Guerrero-Arias, A., Jaramillo-Alcázar, A., & Luján-Mora, S. (2021).

Mobile learning Technologies for Education: benefits and pending issues.

*Applied Sciences*, 11(9), 4111. <https://doi.org/10.3390/app11094111>

Cyber Innovation Center. (2020, June 23). *The state of cybersecurity education*

*in K-12 schools*. CYBER.org. [https://cyber.org/news/state-cybersecurity-](https://cyber.org/news/state-cybersecurity-education-k-12-schools)

[education-k-12-schools](https://cyber.org/news/state-cybersecurity-education-k-12-schools)

Dawson, K., Antonenko, P., Xu, Z., Wusylko, C., & Koh, D. (2022). Promoting

Interdisciplinary Integration of Cybersecurity Knowledge, Skills and Career

Awareness in Preservice Teacher Education. *Journal of Technology and*

*Teacher Education*, 30(2), 275–287.

<https://www.learntechlib.org/p/221089/>

Domeji, Tabitha. (2019). K-12 Cybersecurity Program Evaluation and Its

Application. In BSU Honors Program Theses and Projects. Item 366.

[https://vc.bridgew.edu/honors\\_proj/366](https://vc.bridgew.edu/honors_proj/366)

FBI. (2021, March 17). *IC3 releases 2020 Internet Crime Report*. Federal Bureau

of Investigation. [https://www.fbi.gov/news/press-releases/fbi-releases-the-](https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics)

[internet-crime-complaint-center-2020-internet-crime-report-including-](https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics)

[covid-19-scam-statistics](https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics)

Fouad, N. S. (2022). The security economics of EdTech: vendors' responsibility

and the cybersecurity challenge in the education sector. *Digital Policy*,



*Regulation and Governance*, 24(3), 259–273. <https://doi.org/10.1108/dprg-07-2021-0090>

GenCyber. (2023). *GenCyber FAQs*. <https://www.gen-cyber.com/faq/>

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, 28(3), 81–106. <https://doi.org/10.1080/19393555.2019.1657527>

Javidi, G., & Sheybani, E. (2019). K-12 Cybersecurity Education, Research, and Outreach. *2018 IEEE Frontiers in Education Conference (FIE)*, 3. <https://doi.org/10.1109/fie.2018.8659021>

Joubish, M. F., & Khurram, M. A. (2011). Cognitive Development in Jean Piaget's Work and its Implications for Teachers. *World Applied Sciences Journal*, 12(8), 1818–4952.

Konak, A. (2018). Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students. *Journal of Cybersecurity Education, Research & Practice*, 2018(1). [https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6/?utm\\_source=digitalcommons.kennesaw.edu%2Fjcerp%2Fvol2018%2Fiss1%2F6&utm\\_medium=PDF&utm\\_campaign=PDFCoverPages](https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6/?utm_source=digitalcommons.kennesaw.edu%2Fjcerp%2Fvol2018%2Fiss1%2F6&utm_medium=PDF&utm_campaign=PDFCoverPages)

Kuzmich, E. (2019, September 4). *Children are becoming more vulnerable to cybercriminals as IoT device use explodes*. Open Access Government.

<https://www.openaccessgovernment.org/children-vulnerable-to-cybercriminals/72665/>

Landau, P. (2023, March 22). *What is a stakeholder? Definitions, types & examples*. ProjectManager. <https://www.projectmanager.com/blog/what-is-a-stakeholder>

Laricchia, F. (2022, August 25). *Children with internet access at home worldwide 2020, by region*. Statista.

<https://www.statista.com/statistics/1327322/children-with-internet-access-at-home-by-region-worldwide/>

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176–8186. <https://doi.org/10.1016/j.egyr.2021.08.126>

Lopez, G. A. (2021). *Investigating the Ransomware Infection Rate of K12 School Districts During the Covid Pandemic* (Publication No. 1317) [Master's thesis, California State University San Bernardino]. Scholarworks

Morgan, S. (2022, October 17). *Cybercrime To Cost the World 8 Trillion Annually In 2023*. Cybercrime Magazine.

<https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>

Nakama, D., Pullet, K., & Morris, R. (2018). Solving Problems of Practice to Broaden Participation in Cybersecurity Education. *Issues in Information Systems*, 19(4). [https://doi.org/10.48009/4\\_iis\\_2018\\_1-9](https://doi.org/10.48009/4_iis_2018_1-9)

NIST. (2023). *Social Engineering - Glossary*. Retrieved August 26, 2023, from

[https://csrc.nist.gov/glossary/term/social\\_engineering](https://csrc.nist.gov/glossary/term/social_engineering)

Olmstead, K., & Smith, A. (2017, March 22). *What Americans knows about cybersecurity*. Pew Research Center: Internet, Science & Tech.

<https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/>

OpenAI. (2023). *ChatGPT* (October 26 version) [Large language model].

<https://chat.openai.com>

Pew Research Center. (2019). Climate Change Still Seen as the Top Global Threat but Cyberattacks a Rising Concern. In *Pew Research Center*.

Prior, S., & Renaud, K. (2022). The impact of financial deprivation on children's cybersecurity knowledge & abilities. *Education and Information Technologies*, 27(8), 10563–10583. <https://doi.org/10.1007/s10639-022-10908-w>

ProofPoint. (2023). *What is social Engineering? - definition, types & more*.

Retrieved August 26, 2023, from <https://www.proofpoint.com/us/threat-reference/social-engineering>

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.

<https://doi.org/10.1016/j.ijcci.2021.100343>

- Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, 10(5), 378–382.  
<https://doi.org/10.18178/ijiet.2020.10.5.1393>
- RMC Research Corporation. (2009, November 6). *Engaging Stakeholders: Including Parents and the Community to Sustain Improved Reading Outcomes*. Sustaining Reading First.  
<https://www2.ed.gov/programs/readingfirst/support/stakeholderlores.pdf>
- Santos, H., Pereira, T., & Mendes, I. a. C. (2017). Challenges and reflections in designing Cyber security curriculum. *2017 IEEE World Engineering Education Conference (EDUNINE)*.  
<https://doi.org/10.1109/edunine.2017.7918179>
- Shewale, R. (2023, August 21). *Internet User Statistics In 2023 — (Global Demographics)*. DemandSage. <https://www.demandsage.com/internet-user-statistics/>
- Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, 3(1), 47–67.  
<https://doi.org/10.53889/ijses.v3i1.132>
- Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). Cyber security risks for minors: A taxonomy and a software architecture. *2016 11th International Workshop on Semantic and Social*

*Media Adaptation and Personalization (SMAP).*

<https://doi.org/10.1109/smap.2016.7753391>

Vogels, E., Gelles-Watnick, R., & Massarat, N. (2022, August 10). *Teens, Social Media and Technology 2022*. Pew Research Center: Internet, Science & Tech. <https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>

Yan, Z., Xue, Y., & Lou, Y. (2021, August). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, 121, 106791. <https://doi.org/10.1016/j.chb.2021.106791>