2019-08-01

Cybersecurity Education in Utah High Schools: An Analysis and Strategy for Teacher Adoption

Cariana June Cornel
Brigham Young University

Cybersecurity Education in Utah High Schools: An Analysis and Strategy for Teacher Adoption

Cariana June Cornel

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Justin Giboney
Geoffrey A. Wright

School of Technology

Brigham Young University

ABSTRACT

Cybersecurity Education in Utah High Schools: An Analysis and

Strategy for Teacher Adoption

Cariana June Cornel
School of Technology, BYU
Master of Science

The IT Education Specialist for the USBE, Brandon Jacobson, stated:

I feel there is a deficiency of and therefore a need to teach Cybersecurity.

Cybersecurity is the "activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (NICE, 2018). Practicing cybersecurity can increase awareness of cybersecurity issues, such as theft of sensitive information. Current efforts, including but not limited to, cybersecurity camps, competitions, college courses, and conferences, have been created to better prepare cyber citizens nationwide for such cybersecurity occurrences.

In 2017, a meeting was proposed to discuss cybersecurity training methods for Utah high school teachers. Meeting attendees included the researcher, Brigham Young University Cybersecurity Professor, Dale Rowe, the Alpine IT Career and Technology Engineering (CTE) Program Area Specialist, Karsten Walker, and the IT Education specialist for the Utah State Board of Education (USBE), Brandon Jacobson. However, due to limited budget, resources, and time, few results were achieved since the meeting, including a cybersecurity class certification and offering of advanced cybersecurity related courses on UEN's WebEx Platform (Alpine District only).However, due to limited budget, resources, and time, few results were achieved since the meeting, including a cybersecurity class certification and offering of advanced cybersecurity related courses on UEN's WebEx Platform (Alpine District only).

The research shows that of the 9 school districts reviewed, only 2 of the public high schools taught cybersecurity-focused courses as outlined by the Utah State Board of Education. This is a scarcity that cannot be ignored. There are insufficient offerings of cybersecurity courses in Utah high schools. As a result, Utah is one of the many states unable to fill the shortage of cybersecurity professionals. Thus, this research was conducted to better understand what is inhibiting potential teachers from offering a cybersecurity-focused course. In the hopes of answering the mentioned query, the research involved surveying high school computer teachers about their experience, as well as their perspective on teaching cybersecurity.

Keywords: Utah, high school, teacher, secondary education, Utah State Board of Education, cybersecurity education, CTE, STEM, cybersecurity, security assurance, information security, information assurance, information technology, IT

ACKNOWLEDGEMENTS

I wish to express my sincerest gratitude to my graduate committee chair and professor, Dale Rowe. He has helped and encouraged me with my academics and aspirations since we first met. As my mentor, he has been there to help me finish my bachelors and soon my masters. I experienced and learned so much thanks to his teachings and could never express the amount of gratitude he deserves.

I would also like to express my appreciation to the other members of my committee, Justin Giboney and Geoff Wright, who gave me the utmost patience and guidance. I am grateful to Brandon Jacobson and Ed Mondragon, of the Utah State Board of Education, for their assistance in gathering survey data. I am also appreciative to Victor Villa, of the Utah Open Source Foundation, for allowing me to conduct some of my research at one of his conferences. I would also like to give my thanks to the Utah teachers that helped me; without your willingness to share and respond to my survey there would be no research.

I am most grateful to my family and friends, specifically my sister and parents, for their encouragement, assistance, and support in finishing my education and pursuing my passions.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Background

In 2008, a cyberattack against Heartland, a leading payment systems company, resulted in 130 million compromised records. This attack represented the biggest breach the world had ever seen at the time. Ten years later, a breach on the Marriott Hotel chain resulted in the disclosure of 500 million customer records over a four-year period. The amount of compromised records is almost 4 times (about 3.85) greater than the 2008 incident [1]. The Ponemon Institute indicates that on average, a data breach results in a global loss of 3.86 million USD. Year to year, the average total loss has, and continues to, increase [2]. This value incorporates discovering and responding to the breach, and the subsequent consequences; typical activities include investigation of what caused the data breach, identifying victims of the breach, legal services, communication with victims and the public, lost business with customers, and audit services [3].

A breach is the act of gaining unauthorized access to a restricted space that usually contains sensitive data, such as customer or employee personal identifying information, e.g., Social Security numbers, driver's license numbers, bank accounts, and credit card information. To defend against the loss of such crucial information, it is necessary to practice cybersecurity. According to the National Initiative for Cybersecurity Careers and Studies (NICE), cybersecurity is the "activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or

defended against damage, unauthorized use or modification, or exploitation" [4]. As demonstrated by the breaches listed above, cybersecurity is necessary. Data loss is only one of many harmful consequences a breach could bring. Unfortunately, there is potential for more exploits in the future due to a "rise in reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information" [5, p. 1]. The more numerous and valuable the information stored in the technology, the greater the danger should a breach occur.

Consequently, the reliance on technology and threat of such technology being breached has created a large demand for cybersecurity-aware and cybersecurity-minded individuals. In the United States, "employment of information security analysts is projected to grow 28 percent from 2016 to 2026, much faster than the average for all occupations" [6]. Globally, it was predicted there will be 3.5 million cybersecurity job openings by 2021 worldwide [7]. Unfortunately, the workforce is unable to matchup with the many available cybersecurity jobs, resulting in a predicted global shortage of 2 million [8].

It is crucial for all citizens to become cyber-aware. Practicing cybersecurity leads to a decrease in the risk associated with a compromise [7], [9]. Current efforts to better prepare cyber citizens nationwide include cybersecurity camps, competitions, scholarships, courses, and conferences [10]–[13]. Note that the courses are rarely offered at the secondary level. The IT Education specialist for the Utah State Board of Education (USBE), Brandon Jacobson, said, "I feel there is a deficiency of and therefore a need to teach Cybersecurity." In addressing this need, it is essential for High school students to become cybersecurity aware, otherwise, they will be defenseless against the growing threat of cyber-attacks.

Although there is a curriculum listed on the USBE's website for cybersecurity fundamentals, only 2 high schools of the 9 Utah School districts examined offered these types of courses. While the option of cybersecurity certification is available for study, such as the Certified Information Systems Cybersecurity Professional (CISSP) and Certified Ethical Hacker (CEH), these target cybersecurity professionals; thus, teachers rarely receive these certifications. Additional resources designed for teacher education are limited and unfocused [11], [14]–[16]. There may be an insufficient amount of exposure in college level educator training, inadequate teacher trainings, and even at times, a perceived lack of necessity for cybersecurity [17]. Many professional tests and trainings are also too advanced to use as classroom material at the high school level and instead target college students or professionals. As a result, the lack of high school appropriate teacher training may be one inhibiting barrier to cybersecurity teaching.

To enumerate the situation, in 2017 it was proposed in a meeting between the researcher and Brigham Young University (BYU) Cybersecurity Professor, Dale Rowe, the Alpine IT CTE Program Area Specialist, Karsten Walker, and the IT Education specialist for the Utah State Board of Education (USBE), Brandon Jacobson, that they discuss training high school teachers in cybersecurity. It was theorized that the teachers may not have offered enough cybersecurity courses in the state of Utah as they should be. It was hoped that by encouraging the proliferation of both cybersecurity focused and cybersecurity related courses at the high school level, more students will not only be better prepared to fill the growing need of cybersecurity professionals in the future, but also contribute to a safer, more cyber aware society as well.

Overall, this research was conducted to understand what barriers are potentially inhibiting high school teachers in the state of Utah from offering a cybersecurity-focused course or implementing cybersecurity principles in their current curricula. Hoping to find a solution, the

study involved surveying Utah high school computer teachers about their experience as well as their perspectives on teaching cybersecurity.

1.2 Research Questions and Hypotheses

Q1. What are the barriers that impede teachers from offering cybersecurity-focused courses or including cybersecurity in existing curriculum?

Q2. What is motivating teachers that are currently teaching cybersecurity-focused courses?

H1. Teachers that have the potential to teach cybersecurity-focused courses but are not currently teaching it, is because they feel unconfident.

H2. The teachers that currently teach cybersecurity-focused courses do so because they feel prepared.

H3. A new training program and certification, designed to increase self-confidence and readiness in cybersecurity teaching will increase the feeling of preparedness among teachers.

2 LITERATURE REVIEW

The purpose of this chapter is to provide context for the research. The literature review covers the cybersecurity topics of its: history, significance, extracurriculars, cybersecurity skills, self-assessments, and teacher training.

2.1 History

Whether it is shopping online rather than in a store or sending a text instead of a letter, technology continues to intertwine more with the lives of everyday people. Given that, it is important to recognize the quickly growing demand to be cybersecure. This section will provide a summary of cyber activity and the resulting consequences. Further information will be provided in terms of current and past remediations that occurred as a result.

Indeed, the utilization of technology has increased for the use of entertainment and resources (e.g. search engines, information sites, online shopping). Due to Google being a popular search engine in America, it became a common verb. For instance, "Google it," was a term that may be used to answer questions concerning definitions, tutorials, recipes, and events. Thus, "[T]he reliance on the Internet across the world has created a tech-savvy generation of young people who spend a good deal of their time online… they have grown up with online services such as Facebook, Google, Massively Multiplayer Online Games (MMOG's), online

chatting, and social networks as an integral part of their lives" [18, p. 3]. Because sensitive information such as Social Security numbers, bank account information, and other personally-identifying information is shared for the purposes of creating accounts, posting updates to friends, and shopping, the internet has also become a platform for criminals who wish to extract and exploit that data. Consequently, there is both a rapidly growing demand for cybersecurity professionals in the job market, as well as a level of cybersecurity-awareness individuals in the general population need to reach to prevent such criminal activity.

To prevent or alleviate the possible damage such criminal activity may cause, multiple federal initiatives have been issued and organizations have been created to mitigate such attacks. Examples include NICE, President George W. Bush's Comprehensive National Cybersecurity Initiative, President Barack Obama's Cyberspace Policy Review, and President Donald Trump's National Cyber Strategy (12-14). Each of these initiatives encouraged the use of safe cyber practices and stressed their importance .

2.2 Significance

In today's world, more information, whether that information be financial, personal, professional, or otherwise, is being stored digitally than ever before due to a growing reliance on technology. While this may improve the lives of both businesses and everyday people, few have the skills and training to sufficiently protect themselves against cyber-attacks. According to the International Information Systems Cybersecurity Certification Consortium, Inc. $(ISC)^2$ there is a shortage of approximately 3 million cybersecurity professionals worldwide [22]. Efforts have

been made to train an increasing number of cybersecurity professionals, but there is a still a large projected scarcity in the future.

To put it in another way, it was reported that the ratio of cybersecurity workers to job openings during 2017-2018 was 2:3 in the United States, the ratio being much smaller than the national average for all jobs, 5:8 [23]. This need for more cybersecurity professionals has influenced colleges to offer many cybersecurity courses and degrees, but students should be exposed to cybersecurity at an even earlier stage [17]. Referring to a study released by the Pew Research Center, in 2018 "roughly nine-in-ten teens go online at least multiple times per day" [24, p. 8]. With this amount of exposure, there are many opportunities for teens to fall victim to cyber theft and abuse.

Accordingly, news stories and research studies report, "malware, plagiarism, privacy, and the protection of identity data are only some of the many issues confronting today's school-age children" [17, p. 83]. Although this information was from an article in 2014, the same still holds true and is more relevant 5 years later. The numbers of ways to access the internet has increased, becoming more easily accessible to everyone [24], [25].

Despite so much exposure, not all teenagers know how to protect themselves online. For instance, a Girls Cybersecurity Camp was created at Brigham Young University in 2015 of which thirty-eight female high school students from the Provo, UT area participated. The participants were asked in a pre-camp survey, "How much do you feel you know about cyber safety/cybersecurity?" With a 5-point scale, 1 being nothing at all and 5 being a lot, the average answer was a 2.17. This result was less than satisfying and further suggests there is a need for more cybersecurity education among high school students [26].

2.3 Teacher Training

Multiple methods for the integration of cybersecurity principles have been introduced at the high school level, however, the lack of cybersecurity courses hinders the usefulness of such resources [27]–[29]. Thus, it is important to discuss how to help teachers gain the technical knowledge needed to implement such practices.

Although many approaches have been created, one such paper admitted "The current that [sic] challenge exists in finding engineering faculty and/or teachers that have a deep understand [sic] of security, stay abreast of current security issues, and are able to express such knowledge. to a diversity of non-technical audiences" [29, p. 5]. Unfortunately, not much research has been provided on cybersecurity training for teachers other than the short-term programs where basic cyber safety was usually learned: password strength, public information sharing, cyberbullying, cyber ethics, the importance of firewalls and antivirus, and the like [9], [17], [30].

Correspondingly, a paper focused on measuring the knowledge and preparedness of preservice teachers, people learning how to become certified academic teachers, to teach topics in Cyberethics, Cybersafety, and Cybersecurity (C3). The test contained 75 C3 topics such as exploits, hacking, cyberbullying and copyrights. The results were surprising, as the participants admitted they could "model and teach only 0.05% of the 75 C3 topics" and had "no or uncertain knowledge of 56% of the 75 C3 topics" [17, p. 85]. This data illustrates the need for training preservice teachers.

In like manner, the IT Education Specialist for the USBE, Brandon Jacobson, stated:

> *What we lack is an elevated awareness and knowledge of what is included within a cybersecurity career to resonate with educators, policy personnel, and administrators throughout the districts.*

As a result, it was proposed in a meeting between the researcher and BYU Cybersecurity Professor, Dale Rowe, the Alpine IT CTE Program Area Specialist, Karsten Walker, and Brandon Jacobson, that they discuss training high school teachers in cybersecurity (2017). However, due to limited time and resources, an in-depth cybersecurity teacher training has yet to be fully realized.

2.4 Extracurriculars

While this paper focuses on the necessity of incorporating cybersecurity courses and principles in high school level education courses, it is also important to recognize current extracurricular activities aimed at furthering cybersecurity education.

To illustrate, the GenCyber program commenced in 2014 with the goal of increasing cybersecurity interest and awareness in students and teachers before college. The program consists of three different camps offered over the summer period. The three camps are each dedicated to the K-12 audience comprised of groups of students, teachers, and a combined group of students and teachers respectively [11].

Another example is Cyberpatriot, an organization created to spark new interest in STEM related fields, specifically cybersecurity, at the high school level. The popularity of these programs expanded their reach from the original junior officer air force corps (ROTC) and civil

air patrol (CAP) to up to 500 teams per category with numbers expecting to increase in the coming years [31].

Such projects provide vital teachings and are adaptable as after school/summer offerings. Although they provide enriching opportunities for student learning, these programs are not part of the high school core curriculum or existing computing topics, further emphasizing the necessity for cybersecurity education courses for those unable to participate in such programs.

2.5 Self-Assessments

It is said colloquially that the first step in fixing a problem is to recognize the existence of that problem. This section covers the importance of helping others recognize their level of cybersecurity awareness. A need to identify if there was an existing lack of cybersecurity awareness was recognized. This was determined through subjects assessing their own awareness, acknowledging their confidence in the subject, and answering knowledge questions to affirm the accuracy of their perceived level of awareness. The following articles demonstrate this practice with students and teachers.

The first instance of research is the same as the one mentioned in Section 2.3. This tool is great tool for emphasizing the need to train teachers making it a vital assessment. As its purpose is to assess participants' cybersecurity knowledge and awareness, it has inspired the survey for this thesis due to the types of topics and questions that will best address the associated investigation. Rather than preservice teachers, inservice teachers, teachers currently practicing their profession, will be the subject matter experts and focus for this study.

Another study assessed the cybersecurity awareness of college and high school students. A group of college and high school students took the Cybersecurity Awareness Scores (CAS) test, a method where participants were asked to self-assess their awareness level or concern. Such questions began with "how likely," "how aware," and "how careful". For example, one question asked "how aware are you of the cybersecurity implications of *https:* versus *http:* in a website address" [32, p. 31]. By starting questions in this manner, the researchers were able to comprehend the amount of awareness the participants held in comprehend the amount of awareness the participants held in different cybersecurity practices.

Furthermore, confidence is yet another factor for assessment. Confidence is essential for teachers, as the "Fast-paced changes in the fields of educational policies and practices meant that teaching becomes a subject of 'complex professionalism' (Hargreaves & Goodson, 1996) whereby teachers are required to have the confidence to be willing to take risks and to try out new ideas and strategies in their pedagogic work" [33]. While teachers are expected to follow changes in their field, those that teach cybersecurity will need to address other concerns such as the risk of students behaving maliciously online, breaking systems, and more. Thus, it was imperative that each teacher's confidence be considered in regards to their ability to teach cybersecurity.

For example, a research project used self-efficacy, decision-making, and interests to determine the effectiveness of competitions as a recruitment method. In particular, some questions asked about the level of confidence and comfortability surrounding the participants' cybersecurity knowledge; "if an individual's self-efficacy is much lower than their ability, they may fail to challenge themselves and set goals that are too low. Conversely, if an individual's

abilities are much lower than their self-efficacy, they may set impossible goals and possibly quit when they fail to meet those goals" [12, p. 6]. This statement leads to the idea that leads to the idea that comfortability and confidence are yet another method of self-assessment that can prove vital to furthering a person's cybersecurity learning and ability.

Many classes used tests (e.g. SAT, ACT, GRE, STAR) to determine knowledge gained, current understanding, and if a change of instruction was needed. Thus, rather than asking what participants know about, using tests asked what participants know. This is a large difference, with one being only familiarity with a subject and the other, knowledge. To illustrate, a research study distributed tests to assess knowledge gains from cybersecurity education programs. The researchers asked cybersecurity questions such as "what are three components of information cybersecurity," and "why is patching important." Each question had five answer choices, with "I don't know" as the last option [34]. With this manner of questioning, participants felt less pressured to guess and more prone to admit any lack of knowledge. This type of assessment gave an indication of which cybersecurity principles were not being addressed well or at all.

By understanding and addressing the weaknesses of individuals as they relate to cybersecurity knowledge, trainings may be made or reformed to increase a person's cybersecurity skills and awareness.

3 METHODOLOGY

3.1 Overview

A review of existing research was a key part of understanding how to approach the central problem: *What inhibits teachers from teaching cybersecurity topics?* This problem led to the development of a series of discovery questions to uncover the root cause surrounding the absence of cybersecurity from many Utah high schools.

The queries were distributed via the Qualtrics survey platform to high school teachers in local school districts. The survey utilized qualitative and quantitative questions for the purposes of cross referencing and suggesting correlation. All questions and the taking of the survey were voluntary and mainly distributed via social media and email to high school teachers who teach computer courses.

3.2 Subject Matter Expert Selection

The survey was administered to Utah high school teachers who teach computer courses. The subject population was determined by the following criteria:

1. Being a teacher in one of the following Utah districts: Alpine, Box Elder, Cache County, Canyons, Davis, Granite, Jordan, Logan City, Murray City, Nebo, Salt Lake City, Uintah, or Washington County.
2. The offering of a computer related course or courses.
3. Teaching at the high school level.

"High School" will be referring to grade levels 9-12 or 10-12, depending on the school the teacher works in. "Computer course" refers to courses that teach a computer literacy skill that involves understanding how the computer works or communicates. These courses in the Utah State Curriculum include:

- Computer Technology (1 and 2)
- Web Development (1A, 1B, and 2)
- Technological Literacy
- Computer Programming (Intro, 1, 2, 3, AP, and IB)
- Intro to Information Technology
- Game Design
- Game Development Fundamentals (1 and 2)
- Exploring Computer Science Principles (1 and AP)
- A+ Computer Maintenance and Repair
- Linux Fundamentals – Networking

- Security Fundamentals
- Foundations of Computer Science
- Fundamental Programming
- Object Programming
- Database Development
- Networking +/ Cisco, Security +
- Network Security
- Mobile Development Fundamentals

The districts studied were chosen based on the respondents, their connections, and the researcher's connections and proximity to the teacher training event (further detail provided in Section 3.5). Each subject was given a briefing of the research and an explanation that the survey was a voluntary experience (Refer to Appendix A: Qualtrics Survey).

3.3 Variables

It was necessary to ask about and assess the background of all individuals because the background of each person creates varying perspectives and influences their answers on the survey. This information was used to compare the results in terms of the level of awareness, and then again based on experience.

The International Technology and Engineering Association (ITEEA), the leading organization for technology and engineering educators, published a book of technological

literacy standards (STL) to help facilitate the standard technology knowledge needed for grades K-12. The majority of the teachers surveyed use and or are aware of the STL, so it can be assumed that they understand the need to be technologically literate and to teach technology literacy.

Standard 17 states that "Students will develop an understanding of and be able to select and use information and communication technologies," which includes cybersecurity since the standard is so broad [35, p. 166]. It was necessary to determine if teachers who teach cybersecurity gained cybersecurity knowledge through outside sources or from specific education programs because cybersecurity is not specifically addressed in these standards, and if those who don't teach cybersecurity have any knowledge of the subject.

3.4 Survey

This section will discuss in detail the different parts of the survey: background, potential barriers to teaching cybersecurity, teaching confidence, awareness, knowledge, and follow-up. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, a National Institute of Standards and Technology (NIST) initiative was used to help create the survey questions. Upon completion, the survey was evaluated by cybersecurity and academic professionals, one working at NBCUniversal as an Information Technology Project Manager and then 2 cybersecurity professors with extensive work experience. After gaining approval, the survey was ready to be distributed. Please refer to Appendices A-D for the survey.

3.4.1 Background

To correlate any connections between certain aspects of subjects' background and their answers, it was essential to group the participants. For example, questions regarding the subject's experience with teaching a high school cybersecurity course, certifications held [8,18,26], and cybersecurity principle implementations were used as the basis for forming groups. The teachers were separated into three categories: taught a computer course, taught security-related course, or taught security-focused course. These groupings helped connect the answers to the rest of the survey in regards to the influence of different perspectives.

3.4.2 Course List

The aforementioned categories were formed on the basis of what classes the teachers offered. By creating definitions for the purpose of classification, data could be separated accordingly. Furthermore, this classification enabled the appropriate sampling of subject matter experts.

The courses listed within the survey are cybersecurity-related courses found on the USBE website [37]. The teachers that responded that they taught a cybersecurity course were given the question of which course(es) they taught and would be given this list as choices. These courses were added on the criteria that they reviewed at least one cybersecurity aspect, or had a cybersecurity prerequisite in their Course Strands & Standards or information document. Figure 1 is a decision tree of how courses were chosen. In addition, those with at least three cybersecurity standards were considered cybersecurity-focused courses (see Appendix E for details).

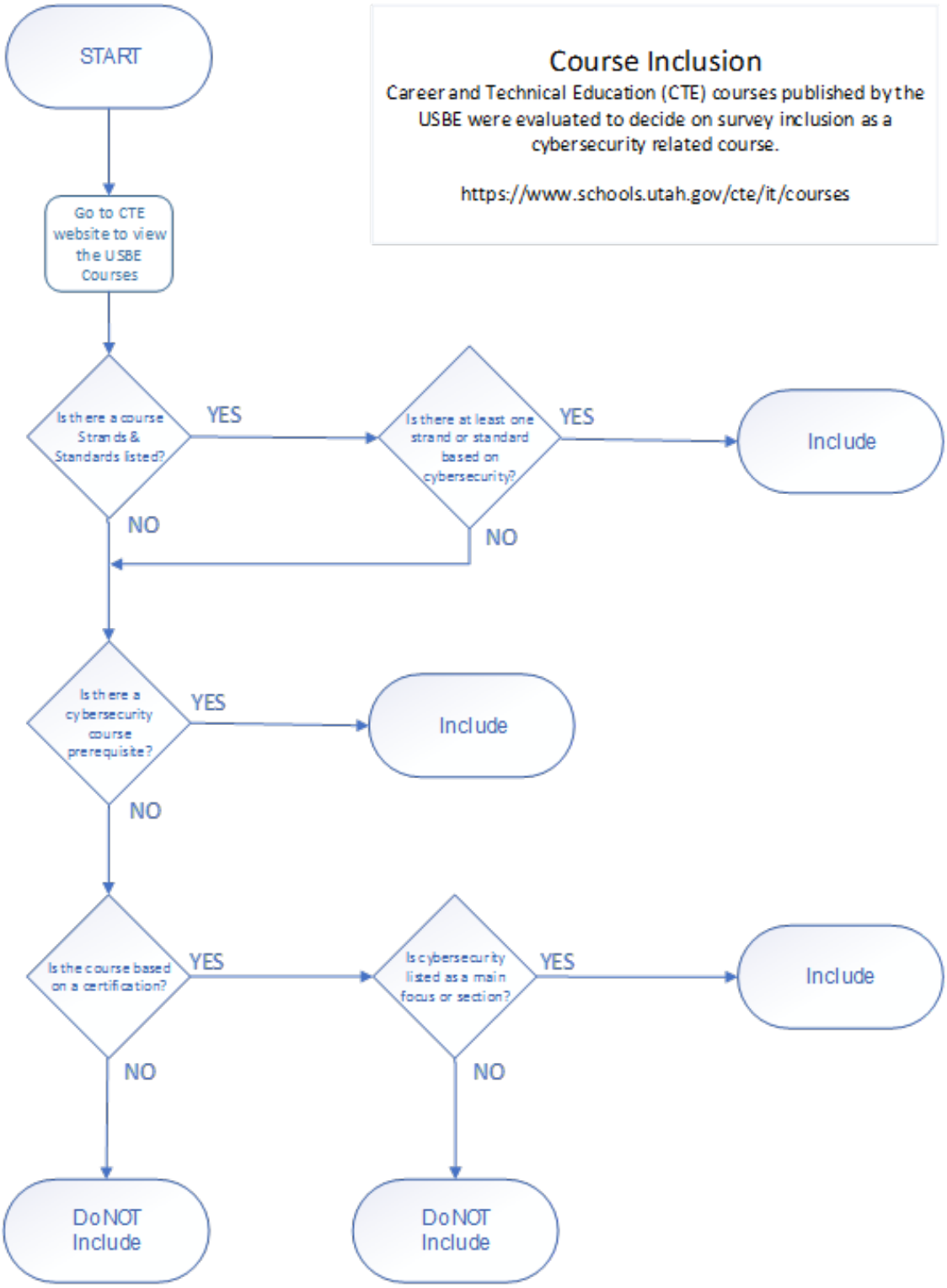


Figure 1: Course Inclusion Decision Tree. The decision tree guides on whether or not the USBE course can be classified as a security related course.

3.4.3 Potential Barriers to Teaching Cybersecurity

This section gathered the collective teacher understanding of what prevented teachers from teaching cybersecurity or what encouraged teachers to teach cybersecurity courses. To this end, teachers were asked what barriers, if any, they think exist that prevent more cybersecurity courses from being offered in the state. The answer can help determine the problems and help find solutions that would encourage more offerings of cybersecurity-focused courses. As these inquiries were very similar, this helped reconfirm their answer to the first.

3.4.4 Teaching Confidence

The purpose of this section was to determine the teachers' level of confidence in their content knowledge as well as their teaching ability. The self-confidence questions were included as a way to link backgrounds with confidence. Therefore, the questions asked teachers how confident they felt in teaching cybersecurity as a course or implementing the principles in a security-related course. The teacher's responses about their level of confidence in the material were used to determination if their self-confidence had any relation to their level of implementation. The questions used were taken from a research paper that studied how well self-efficacy and other abilities predict the effectiveness of cybersecurity competition participants [39].

3.4.5 Cybersecurity Awareness

Cybersecurity awareness was another topic that was used to investigate any relation to the other sections. By doing this, it is possible to understand the current awareness level of the participants. The awareness level was assessed through questions beginning with "how likely,"

"how aware," "how careful," and "how concerned." These questions asked about cybersecurity practices in everyday life [32].

3.4.6 Cybersecurity Knowledge

Knowledge-level questions determined how much the teachers already knew about cybersecurity. Their knowledge was assessed based on the accuracy of their answers to each knowledge question [34]. Their answers allowed us to investigate the possibility that confidence could be linked to how knowledgeable an individual is with regards to cybersecurity.

3.4.7 Follow-Up

Finally, there were follow-up questions. The questions asked if there was any additional information the participants would like to share and if they'd be willing to give further clarification on their response if needed.

3.5 Method of Distribution

The survey was voluntary, with each question being optional. How many subjects were willing to take the survey and then share the survey with other Utah technology teachers determined how much the survey was shared. Surveys were distributed online via email, social media, Quick Response (QR) code, and a website address. The QR code was distributed during a two-day Utah cybersecurity teacher training at a cybersecurity conference in April of 2019. In addition to being shared online, the website address was shared during the same teacher training.

4 ANALYSIS

4.1 Overview

This chapter focuses on answering the research questions and theses (Section1.2), in addition to significant findings. Data gathered from Utah computer teachers supported the answers based on the criteria listed in Section 3.2. The population was broken down into groupings of computer teachers that teach the following types of course(s): security focused, security related, and non-security course. The data was analyzed using these course groupings to compare and contrast results. The overall results helped validate and answer the hypotheses and questions mentioned in Chapter 1.2.

4.2 Population Representation

As it was difficult to receive the necessary statistics from the Utah State Board of education, the process was undertaken by the researcher, using open source intelligence. The following Utah Districts were picked based on proximity to criteria listed in chapter 3.2: Alpine, Box Elder, Cache County, Canyons, Davis, Granite, Jordan, Logan City, Murray City, Nebo, Salt Lake City, Uintah, and Washington County. The school websites, found in the Utah Schools Directory, were used to identify the teachers and the class(es) they taught [40]. However, due to the general unavailability of information on many school websites, the following districts were excluded from this data: Box Elder, Davis, Logan City, and Uintah.

Additionally, some of the respondents that took part in the survey did not teach at a public school. In order to utilize and better organize the statistics, their data was included as part of the population of the school districts where they would geographically belong.

Of the chosen districts, 68 teachers taught a computer related course. Of those teachers, one taught only security focused courses (1.5%) and 48 taught cybersecurity-related courses, which is roughly 70.6%. Furthermore, of these 48 teachers, six of them also taught cybersecurity-focused courses, about 9.9% of the total computer teachers. The rest of the computer teachers (27.9%) did not teach cybersecurity at all. For easier visualization, a breakdown can be seen in Figure 2.

With a population size of 68, confidence level of 90%, and sample size of 31, the margin of error is 11% [41]. Thus, 90% of the time the opinions in this research will be within 11% of the opinion of the overall population.

Population (P) = 68

Sample size (s) = 31

4.3 Review of Research Questions and Hypothesis

Q1. What are the barriers that impede teachers from offering cybersecurity-focused courses or including cybersecurity in existing curriculum?

Q2. What is motivating teachers that are currently teaching cybersecurity-focused courses?

H1. Teachers that have the potential to teach cybersecurity-focused courses but are not currently teaching it, is because they feel unconfident.

H2. The teachers that currently teach cybersecurity-focused courses do so because they feel prepared.

H3. A new training program and certification, designed to increase self-confidence and readiness in cybersecurity teaching will increase the feeling of preparedness among teachers.

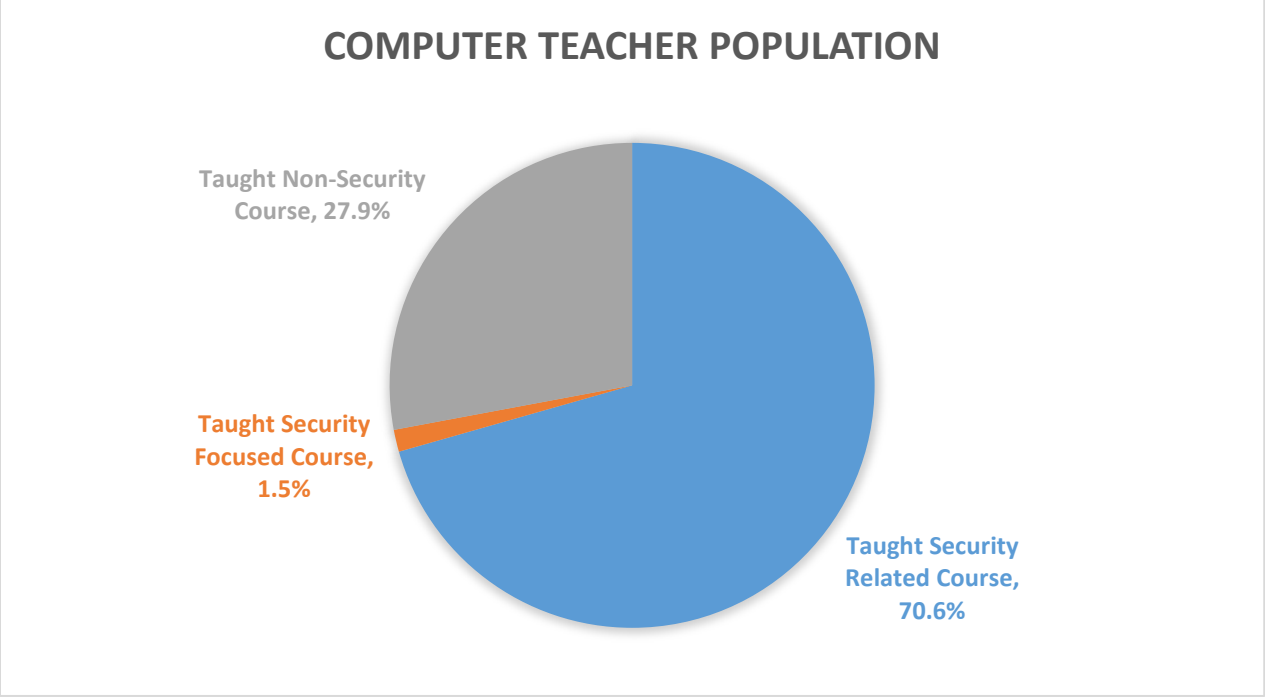


Figure 2: Computer Teacher Population. The figure shows what portion of teachers taught a course in regards to cybersecurity-focused, cybersecurity-related, and non-security courses.

4.3.1 Answering and Validating Research Question 1 (Q1)

Survey Question 6:

What barriers do you think are blocking high school technology teachers from implementing cybersecurity principles in their courses?

Question 6 gave the teachers nine options to choose from, of which they could choose more than one answer: wages, class size, school institution does not offer enough support, lack of cybersecurity teaching resources, teachers' lack of interest, students' lack of interest, lack of funds, there are no barriers, and other. Question 6 was included due to a desire to learn what was discouraging teachers from implementing cybersecurity principles in their courses. The answers were potential factors gathered from observation around technology teachers, experience with the annual Girls Cybersecurity Camp (GCC), and the technology education courses required for the Technology Engineering Studies bachelor's degree.

According to the high school educators surveyed, the main barriers to teaching cybersecurity principles in their classrooms are the lack of cybersecurity teaching resources (Option 4, 67.7%) and a lack of support from the schools (Option 3, 54.8%). This difference can be seen in Figure 3.

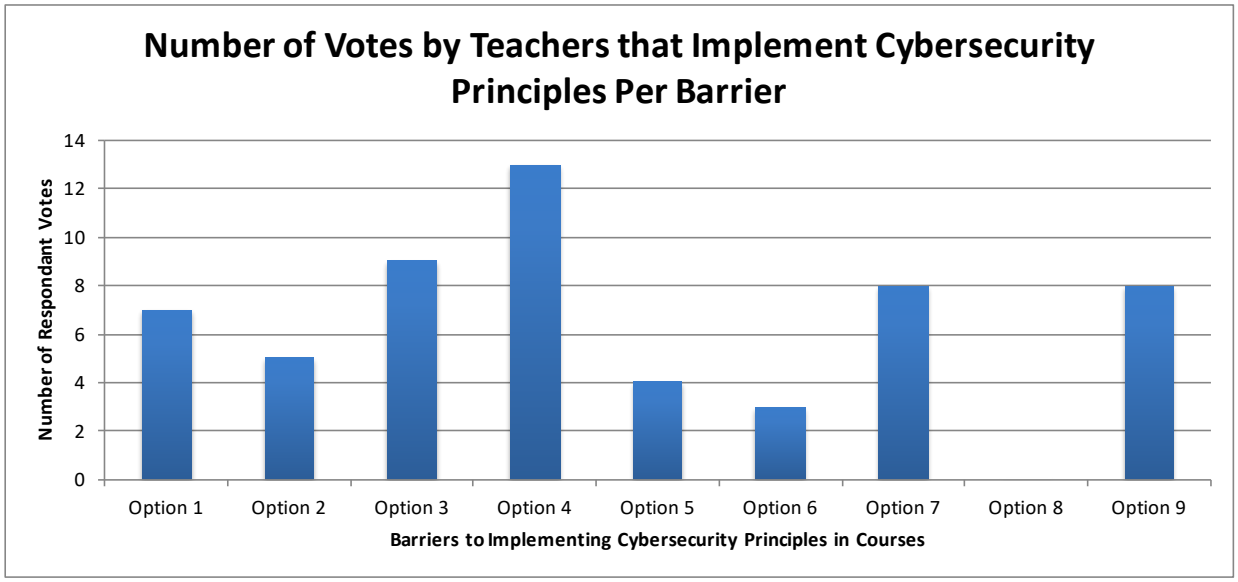


Figure 3: Number of Votes by Respondents vs. Barriers to Implementing Cybersecurity Principles in Courses

Thus, the top two answers for Q1 are the lack of support from schools and a lack of cybersecurity teaching resources. Unfortunately, these barriers had no significance when compared to how many cybersecurity principles were taught (Table 1, Figure 5). For instance, figure 5 shows the relationship between the barrier, "School/Institution does not offer enough support" versus the number of cybersecurity principles teachers included in their curriculums. However, there appears to be about an equal number of teachers that agree (a 1 on the x-axis) and those that disagree (a 0 on the x-axis). If these barriers were significant compared to the number of security principles taught, they would correspond to a lower number of cybersecurity principles taught. Even though there was no statistical significance, this finding suggests that all teachers tend to agree on which barriers are more prevalent. Thus, the barriers found are important; they illustrate how teachers feel, which can affect how they teach.

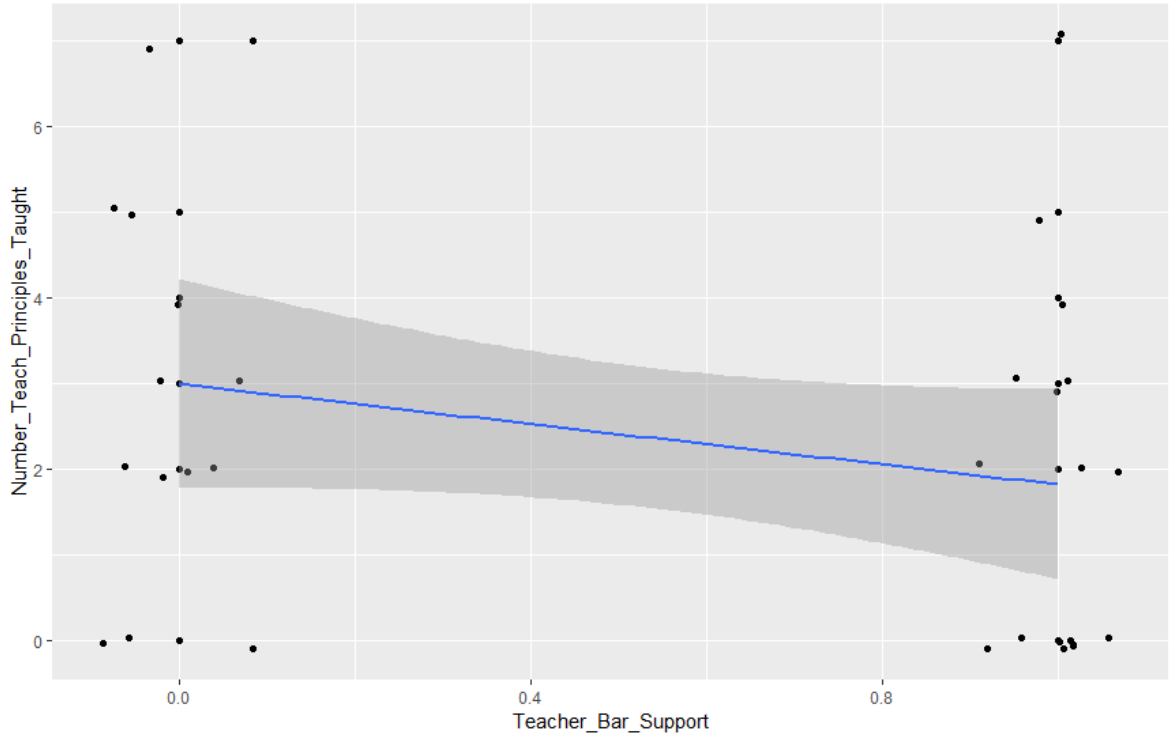


Figure 4: Linear Regression graph of School/Institution Does Not Offer Enough Support vs. Number of Cybersecurity Principles Taught.

Table 1: Linear regression of the potential influencers of how many cybersecurity principles are taught.

```
Coefficients:
                                  Estimate     Pr(>|t|)
(Intercept)                        15.8010     0.0234 *
CONFIDENCE_TEACH_CYBERSEC_TOPICS   -0.6159     0.0507 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

The participants that checked “other” had some other potential barriers to consider. These answers included the following:

Too high a barrier to entry for regular teachers. You might train a run-of-the-mill teacher to do web development or light programming, but for cyber, you need to pull people from industry. And nobody wants to take that pay cut.

Teacher knowledge. I don't know wtf I am doing.

Generally [sic] without state level approved courses and strands-standards we are not allowed to teach items not approved at state level.

Time involved in preparing to teach another class when I'm already teaching 5 different IT courses.

Time...adding one more thing to a curriculum already over-stuffed with state-mandated performance objectives.

The district will not offer more types of computer courses when there are other options (i.e. web development, programming, gaming fundamentals, etc.) which are not full.

These answers mainly focus on lack of knowledge, district offerings, exclusion from class Strands and Standards, and insufficient staffing for cybersecurity. In considering the approach for fixing these barriers, these should be taken more into account as many others may agree.

4.3.2 Answering and Validating Hypotheses 1 and 2 (H1 & H2)

Survey Question 11

In general, how confident are you about your ability to teach cybersecurity/information assurance topics?

Survey Question 12

In general, how comfortable are you with your level of knowledge to teach cybersecurity/information assurance topics?

Comfortability and confidence are very important aspects of teaching [17], [33]. Due to this, it was necessary to assess these traits. The results, as represented in Table 2, suggest that there is a strong correlation between a teacher's confidence in their topic knowledge and their confidence in their teaching ability. Furthermore, teachers that expressed confidence in question 12 admitted near the same level of confidence in question 11. However, there is an exception: some teachers said they were somewhat unconfident for question 12.

Half of them expressed the same level of "somewhat unconfident" in question 11, but the rest expressed that they were somewhat confident in their ability to teach cybersecurity. Our interpretation of the data presented in the aforementioned table is that a teacher's confidence in their ability to teach cybersecurity tends to be the same as their confidence in their knowledge of the subject. Where they differed in their answer, the confidence in their knowledge tended to be one level lower than their confidence in their ability to teach.

Table 2: Relation of confidence levels in regards to survey questions 11 and 12.

	Q12: In general, how comfortable are you with your level of knowledge to teach cybersecurity/information assurance topics?					
Q11: In general, how confident are ...	Confident	Somewhat confident	Somewhat unconfident	Neither confident nor un...	Not confident	Total
Confident	100%	0%	0%	0%	0%	100%
Somewhat confident	7.7%	76.9%	15.4%	0%	0%	100%
Neither confident nor unconfident	0%	33.3%	0%	66.7%	0%	100%
Somewhat unconfident	0%	0%	66.7%	33.3%	0%	100%
Not confident	0%	0%	0%	0%	100%	100%
Total						

Furthermore, a majority of the participants (51.7%) said they were either confident or somewhat confident in question 11 and confident or somewhat confident in question 12. This data suggests that most teachers have some level of confidence in both areas. Further analyzing the data, a linear regression was used to determine if any correlation exists between confidence and the number of cybersecurity principles taught. Figure 6 shows that the confidence level had a statistical significance on the confidence in teaching cybersecurity topics (0.0507). The graph shows that the more confident a teacher is in teaching a topic, the more cybersecurity principles they tend to teach (Table 3, Figure 6).

The correlation of this data, and the conclusions drawn from them, suggest that as a teacher becomes more confident in his or her knowledge of cybersecurity, the confidence in their ability to teach the given topic increases. Thus, the teachers' confidence level is vital for teaching cybersecurity, **validating H1** and **H2**.

4.3.3 Answering and Validating Research Question 2 (Q2)

Only 2 of the 31 teachers surveyed currently teach, or taught, at least one high school cybersecurity course within the last year (Survey Question 1), representing only 29.6% of the Utah high school educators that offer cybersecurity-focused courses. In terms of answering Q2, these two respondents were encouraged to teach cybersecurity due to previous experience or that it was "fun and applicable" (Survey question 2).

However, there were too few of these educators, making it difficult to reach more of these respondents. In order to more accurately answer Q2 with a proper representation, all the respondents' answers had to be taken into consideration. Thus, Q2 needed to change to: What is motivating teachers to teach cybersecurity principles in their courses? As a result, survey question 7 was asked:

Survey Question 7

What do you think would encourage high school technology teachers to implement cybersecurity principles across the curriculum? (Multiple Choice)

This inquiry gave the teachers the following 6 options to choose from, and they were allowed to choose more than one answer: pay raise, school/institution support, cybersecurity teaching resources, sufficient funds, teacher training, and other. The two most popular answers to survey question 7 were Teacher Training (Option 5, 90.3%) and Cybersecurity Teaching Resources (Option 3, 77.4%). These numbers, along with the responses from survey question 6, suggest that technology (computer) teachers don't feel like there is enough training, resources, and structure in place to facilitate teaching cybersecurity. A breakdown of these responses can be found in Figure 8. Of those that answered "other", some of the results mentioned the following:

The curriculum would need to be updated to include cybersecurity.

This is very much similar to one of the answers given as a barrier in Section 4.3.1. Though these answers are telling, just looking at the chart was not enough. Further analysis required the use of linear regression to check if any correlation exists between what teachers saw as the incentives to implement cybersecurity principles and the number of cybersecurity principles those teachers taught (Table 4). Examining Figure 8 and Table 4, the encouragement shows no

significance on how many cybersecurity principles were taught. Therefore, we can say that what teachers see as incentives had no effect on how many cybersecurity principles were taught. While there was no statistical significance in this data set, these answers are still important. Similar to Q1, they illustrate how teachers feel which can affect how they teach, and it is suggested that further research be done to determine if any correlation exists.

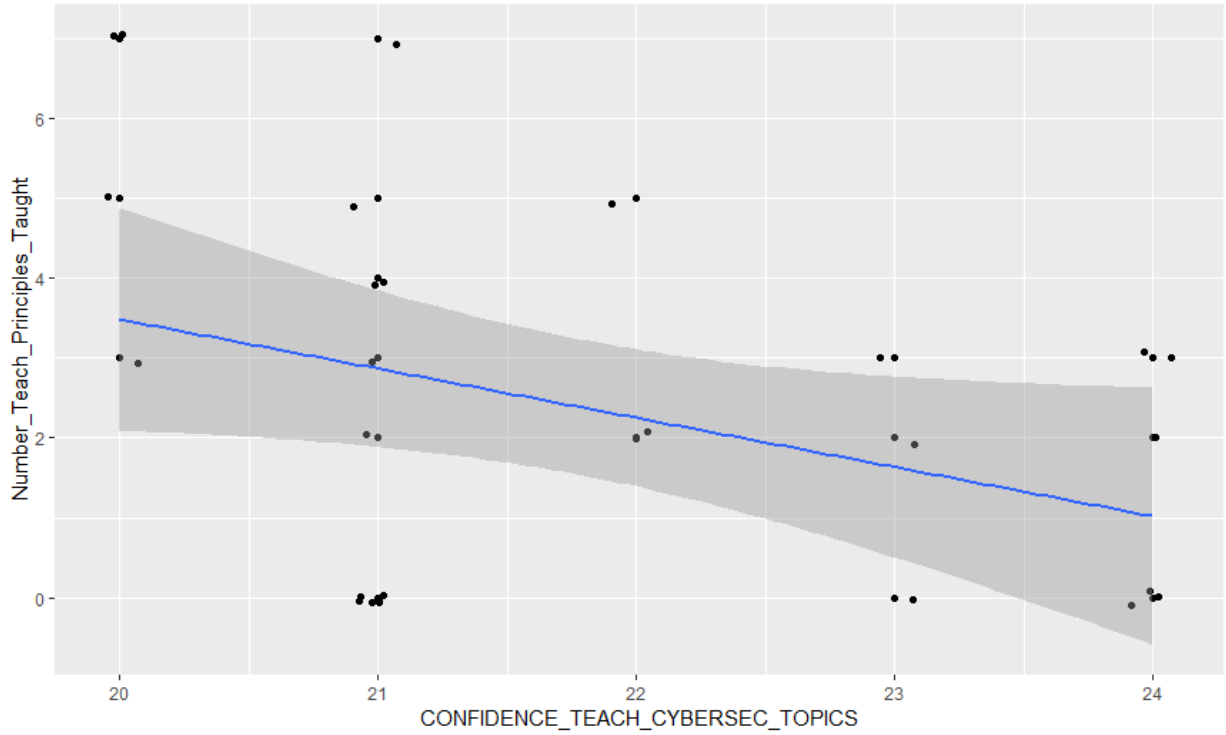


Figure 5: Linear Regression graph of *Confidence in Ability to Teach Cybersecurity/Information Assurance Topics* (20 being confident and 24 being not confident) vs. *Number of Cybersecurity Principles Taught*

Table 3: Linear regression of confidence as a potential influence on how many cybersecurity principles are taught

```
Coefficients:
                                 Estimate     Pr(>|t|)
(Intercept)                       15.8010      0.0234 *
CONFIDENCE_TEACH_CYBERSEC_TOPICS  -0.6159      0.0507 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

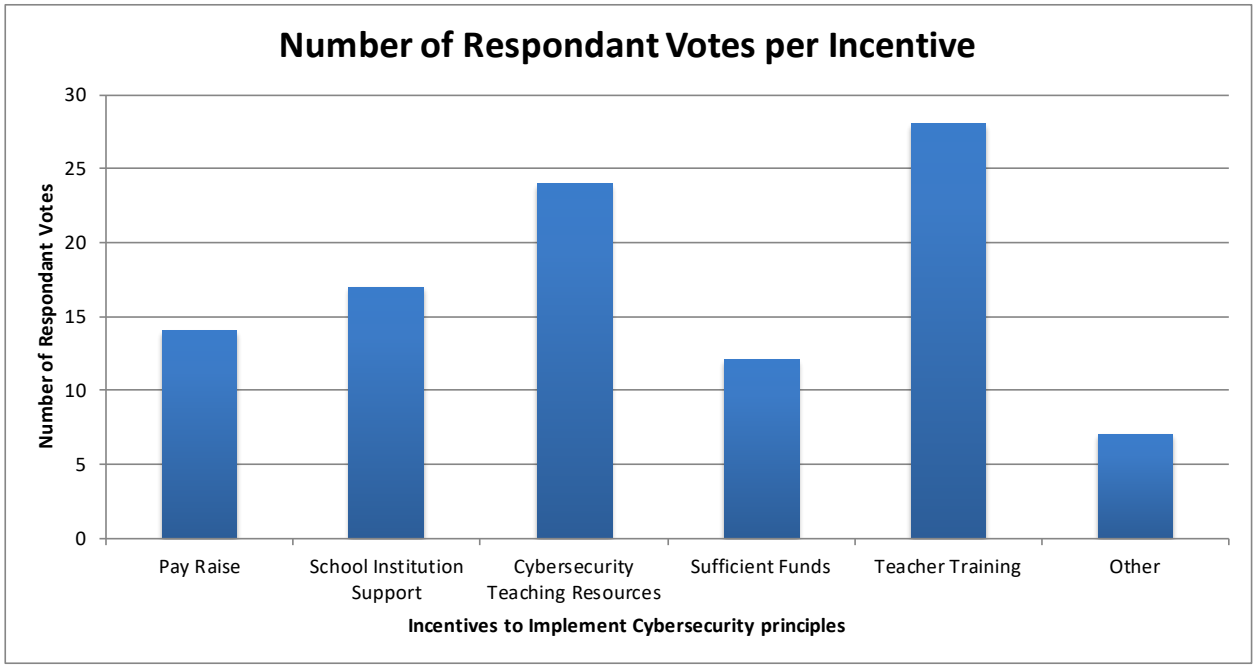


Figure 6: Number of Respondent Votes per Incentive to Implement Cybersecurity Principles

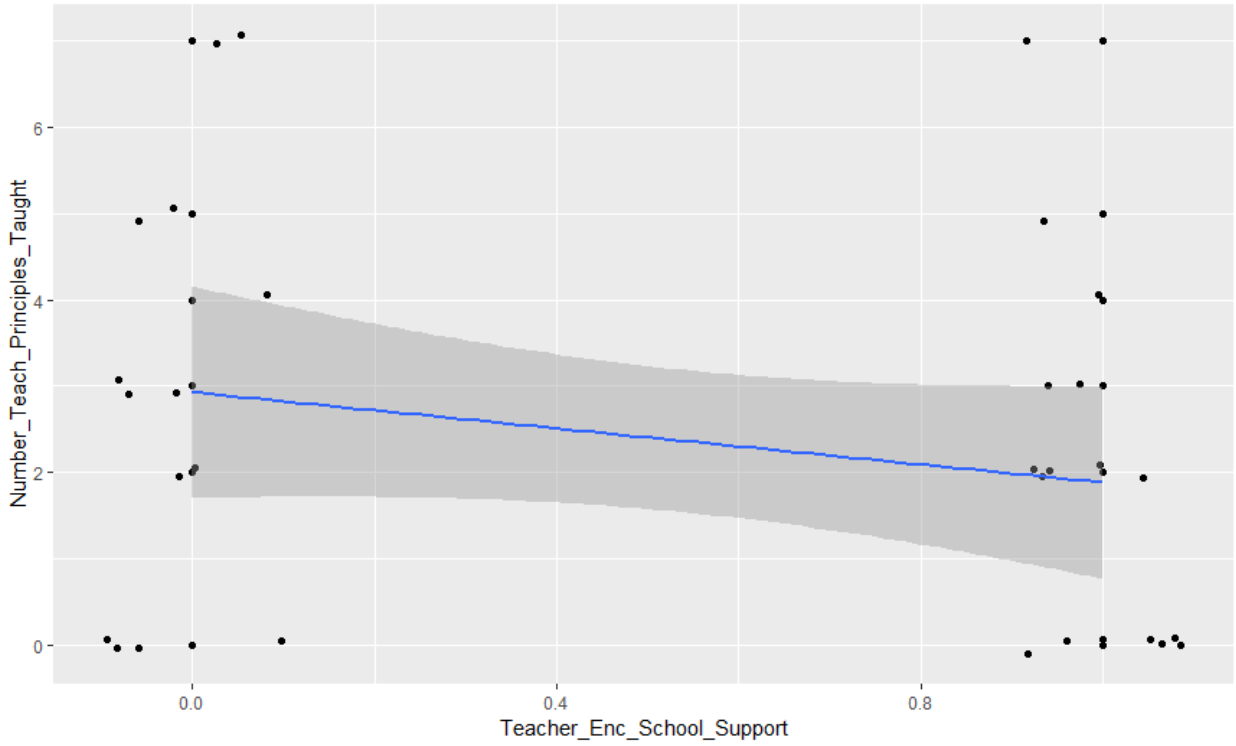


Figure 7: Linear Regression graph of *School/Institution Support* (1 being the respondent believed this would help) vs. *Number of Cybersecurity Principles Taught*

Table 4: Linear regression of different encouragements as potential influencers of how many cybersecurity principles are taught

```
Coefficients:
                              Estimate Std. Error t value Pr(>|t|)
(Intercept)                     2.2372     1.5867   1.410    0.171
dat$Teacher_Enc_Pay_Raise       0.2845     0.9899   0.287    0.776
dat$Teacher_Enc_School_Support -1.2975     1.1193  -1.159    0.258
dat$Teacher_Enc_RSS            -0.1619     1.1756  -0.138    0.892
dat$Teacher_Enc_Funds          -0.1031     1.0686  -0.097    0.924
dat$Teacher_Enc_Teach_Training  1.0672     1.5841   0.674    0.507
dat$Teacher_Enc_Other          -0.4335     1.2193  -0.355    0.725
```

4.3.4 Answering and Validating Research Hypothesis 3 (H3)

Answering Hypothesis 3 was not integrated well into the methodology. Thus, anecdotal evidence was used to answer H3.

Through my own experience as a cybersecurity and teaching expert, I experienced both perspectives. Through observation and conversation with high school technology teachers, I noticed that teachers were bored of learning about the basics of cybersecurity, such as ethics, password safety, social engineering, and online safety.

For instance, during the cybersecurity teacher training at the security conference mentioned beforehand, I taught ethics and social engineering on the first day. Throughout the day, one of the teachers continuously asked "when are we going to do something technical?" Apparently, a lot of them had been attending cybersecurity teacher trainings but were commonly taught the same basics: password strength, ethics, and social engineering. There was often little to no opportunity for technical training. To emphasize, one participant reported:

> *Cybersecurity has always been a mystery. The USBE trainings I've attended at summer con[ff]erence [sic] (usually the LDS Business College guy) are generic with no actual practice / application time. I'd like to learn the general principles AND the most common software used. Thank you!*

On the second day, I conducted a lab on forensics and networking. They tremendously enjoyed taking a more technical approach and asked many questions. At the end, they asked for copies of the labs and presentations for the purpose of using them in their own class or review.

These teachers and others I spoke with and observed were eager to learn about cybersecurity and the prospect of a more technical, hands-on training for teachers, as they "will take care of the teaching part". Hence, a new training program designed to increase self-

confidence and readiness in cybersecurity teaching will increase the feeling of preparedness among teachers.

4.4 Statistical Techniques

Data was analyzed by the Qualtrics Analytics Tool, which used the Chi-Squared Test. The statistical significance was measured using Linear Regression and calculated by the software, RStudio.

In terms of the results used for survey question 5, "What security principles do you currently include, or have previously included, in your curriculum? Please select all that apply," only those who answered they teach cybersecurity principles were given this question. However, because the survey path did not show this question to those that taught a cybersecurity course, they were added to the current data as having taught all the choices (7 total).

4.5 Answers to Research Questions and Hypotheses

Q1: The top two barriers are the lack of support and lack of cybersecurity teaching resources.

Q2: The top two encouragements for the implementation of cybersecurity principles across the curriculum are Teacher Training and Cybersecurity Teaching Resources.

H1 & H2: As a teacher becomes more confident in his or her knowledge of cybersecurity, the confidence in their ability to teach the given topic increases. Thus, the teachers' confidence levels are vital to teaching cybersecurity.

H3: A new training program designed to increase self-confidence and readiness in cybersecurity teaching will increase the feeling of preparedness among teachers.

4.6 Significant Findings

4.6.1 Incentives and Barriers to Teaching Cybersecurity Principles

The top two barriers are the lack of support and lack of cybersecurity teaching resources. Two possible solutions are Teacher Training and Cybersecurity Teaching Resources. Please refer to Chapters 4.3.1 and 4.3.3 for further details.

4.6.2 Cybersecurity Principles Currently Taught

Of the teachers that do not teach a cybersecurity-focused curriculum, 58.6%, implemented cybersecurity principals in their classes within the preceding year. Online safety and password cybersecurity are the top two cybersecurity principals they've incorporated into their curriculums at 58.1% and 51.6% respectively (Figure 9). This shows that there is a rudimentary emphasis for safety among computer teachers that don't teach a cybersecurity-focused curriculum, but more advanced topics are not as widely covered.

4.6.3 Analysis of Knowledge Questions

The amount of correct answers for the three knowledge questions (Survey Questions 17 – 19) were compared to see how knowledgeable in cybersecurity the participants were. Of the participants, 10% correctly answered all the questions, 24 % correctly answered two of the questions, 38% correctly answered one of the questions, and the rest (31%) answered none of the questions correctly (Figure 10). Clearly, not many were able to correctly answer one or two of the questions, illustrating a general lack of cybersecurity knowledge among these teachers and emphasizing the need for more training.

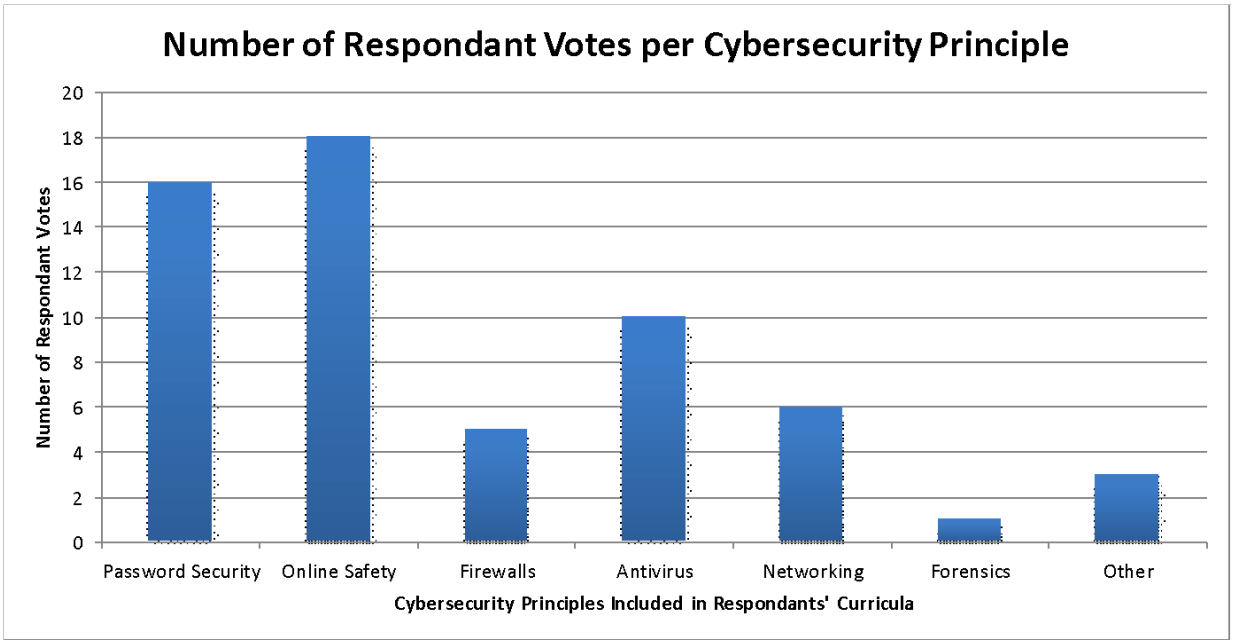


Figure 8: Number of cybersecurity principles that are included in the respondents' curricula.

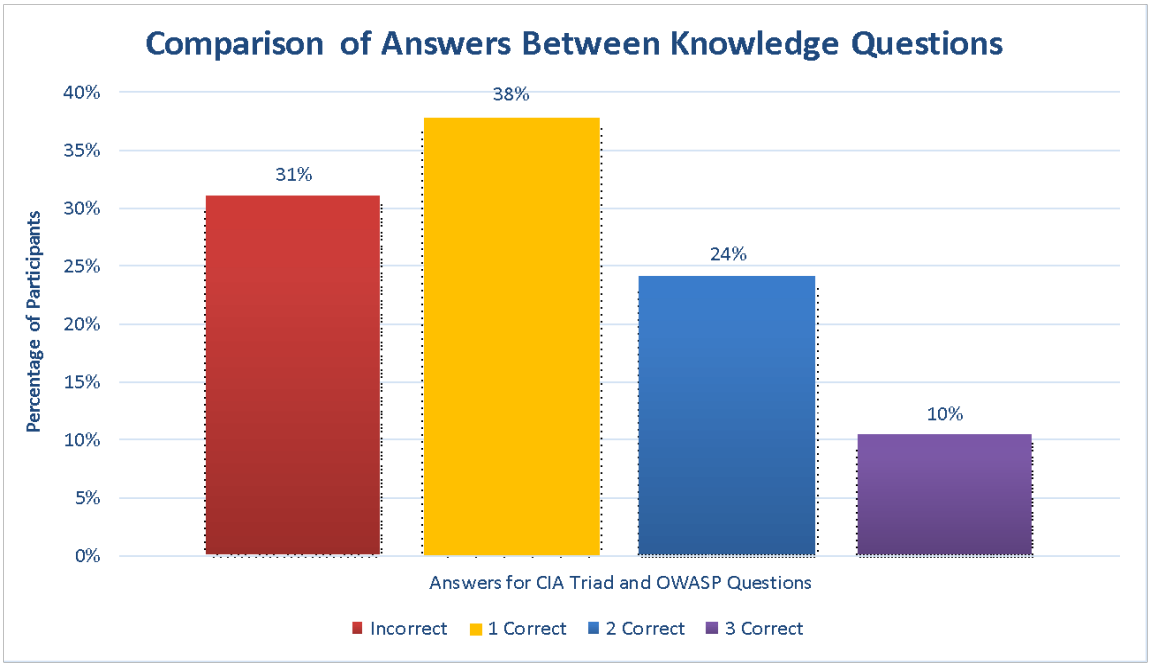


Figure 9: Percentage of participants per total correct answers.

Moreover, a linear regression checked if any correlation exists between answering survey question 18 correctly and the number of cybersecurity principles taught (Table 5). Figure 10 and Table 5 clarify that question 18 was significant (0.00167) when compared to how many cybersecurity principles were taught. Teachers that answered question 18 correctly tended to teach more cybersecurity principles in their courses, and participants that answered the question incorrectly were more likely to teach fewer cybersecurity principles. It is noteworthy, however, that those who answered incorrectly ranged from 0 to 7 security principles taught while those who answered correctly ranged from 5 to 7 principles taught.

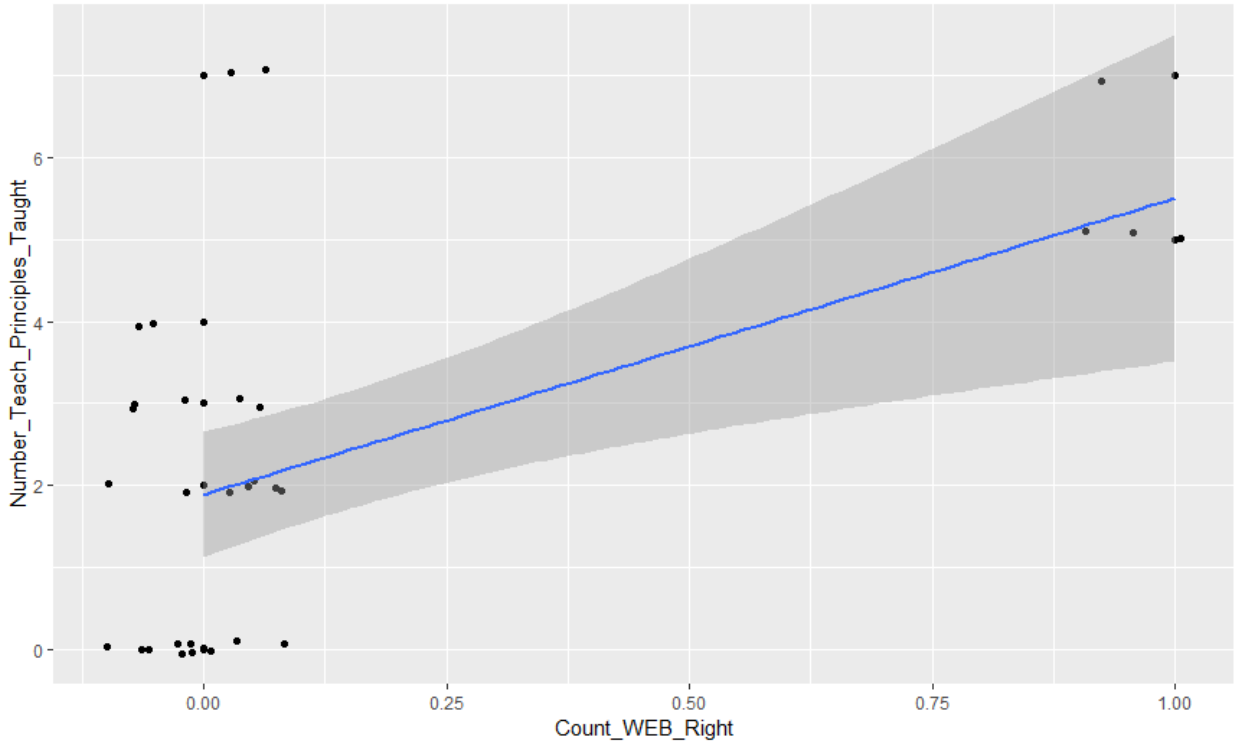


Figure 10: Linear Regression graph of *What is the best-practice standard for secure web application development?* (with 1 being the question was answered correctly) vs. *Number of Cybersecurity Principles Taught*.

Table 5: Linear regression of the answer to *What is the best-practice standard for secure web application development?* as a potential influencer of how many cybersecurity principles are taught

```
Coefficients:
                Estimate Std. Pr(>|t|)
(Intercept)       1.8889     2.22e-05 ***
Count_WEB_Right   3.6111     0.00167 **
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

5 CONCLUSIONS

5.1 Summary

The research appears to indicate that while most computer teachers feel confident in their knowledge and ability to teach cybersecurity, further training is needed. Likewise, many of the respondents indicated that the most pronounced barriers are lack of cybersecurity teaching resources and the lack of support from the schools. They also hold that proper teacher training and resources would be the most impactful incentives for the implementation of cybersecurity courses, above even increased pay. These results can be used to draw the following conclusions to my research questions and hypotheses:

Q1: The top two barriers are the lack of support and lack of cybersecurity teaching resources.

Q2: The top two encouragements for the implementation of cybersecurity principles across the curriculum are Teacher Training and Cybersecurity Teaching Resources.

H1 & H2: As a teacher becomes more confident in his or her knowledge of cybersecurity, the confidence in their ability to teach the given topic increases. Thus, the teachers' confidence levels are vital to teaching cybersecurity.

H3: A new training program designed to increase self-confidence and readiness in cybersecurity teaching will increase the feeling of preparedness among teachers.

After further analysis, the following topics showed statistically significant results: the barriers and incentives to teaching cybersecurity principles, which cybersecurity principles are taught the most, and how well teachers understand cybersecurity. It is worth noting that among computer course teachers, the importance of online safety and password cybersecurity is apparent and shared, whereas the other aspects of cybersecurity are largely untouched. It can be inferred that with standardization of teaching practices and curriculum, more Utah teachers will be able to better educate the youth on proper cybersecurity practices in the future.

5.2 Discussion

Through my own experience as a cybersecurity and teaching expert, I came across the difficulties of both worlds. Through observation, I saw both teachers and high school students become engaged and excited about learning cybersecurity. However, there was also the fact that students lacked knowledge on the topic beyond what they might see in a movie. Furthermore, teachers and students appear to be bored of learning about the basics of cyber safety (such as ethics and password safety) and yearn for more technical training. In fact, at the teacher training where some survey data was gathered, teachers voiced their desire for more technical trainings rather than just learning about the topics aforementioned. They were excited about the possibility of practicing the knowledge content rather than learning how to teach it. By expanding their knowledge, they hoped to implement it in their own teaching style for their own classrooms.

5.2.1 Delimitations

Some challenges faced were finding computer teachers willing to take part in the research and finding out the population size.

Because the data was mostly distributed via respondents (those that took the survey were asked to pass it along to their contacts), there was a chance that the sample size would not be large enough to be representative of the population because the data was mostly distributed via respondents (those that took the survey were asked to pass it along to their contacts). An insufficient sample size was a point of stress, as all the focus while distributing the survey was on getting as many participants as possible. Furthermore, the USBE did not have a public record of the population size. Thus, much time was spent searching through multiple websites to find the number of computing teachers in several districts. Furthermore, there weren't many teachers that taught cybersecurity-focused courses, which caused me to reevaluate how I could answer my hypotheses and research questions.

5.2.2 Risks

There are potential risks that may also be barriers that were not mentioned in the survey. Other risks include losing the teachers to higher pay in industry and the fact that students may hack for malicious purposes. Because teachers can make more money in industry, there is a chance they will leave academia. Some participants reported:

> I am sure pay is important in that anyone that knows much about cyber security would be out making a WHOLE LOT more doing it than teaching it. Teacher training would require funds.

> *You might train a run-of-the-mill teacher to do web development or light programming, but for cyber, you need to pull people from industry. And nobody wants to take that pay cut.*

This risk stems from the fact that once teacher trainings are created and put in place, another barrier, pay, will become more important. If they receive the education needed for the industry,

economically there is nothing stopping them. Further concern is the fact that students may misuse the education for illegal activities. One teacher stated:

> *We used to offer cybersecurity classes, but a student stole a bunch of software and sold it online and got punished by the federal government. So that added to my lack of interest. I don't think it is a good idea to give students access to anything important.*

The teacher's experience greatly discourages the thought of teaching cybersecurity. However, by using certain practices, illegal activities by the students may be limited if not avoided. Practices include teaching Cyberethics, signing ethics agreements, and following case studies [9], [17], [42]. Cyberethics are the morals of using technology such as "copyright, online etiquette, hacking, and online addiction(s)" [17, p. 82]. By using these safe practices, it can be less unnerving when confronted with teaching cybersecurity.

5.2.3 Future Research

In the future, it would be beneficial to replicate the experiment with a bigger sample size and a more accurate account of population size. The survey questions would less be assuming (what barriers are there vs. do you believe there are barriers), include other queries such as "what is keeping you from teaching cybersecurity in your courses" and "why do you want to teach cybersecurity", further filtering participants by asking "what class(es) do you teach/plan to teach", and defining the vocabulary used such as "school support" and "teaching resources". Moreover, the barriers would include the aforementioned risks (Section 5.2.2) in addition to the previous choices. After analyzing survey results, the next step is using the conclusions for the creation of teacher trainings, different lesson plans, and teacher resources to test over a 3-5-year period. Course offerings, teacher population, and student scores would be some of the measurements taken to evaluate the success of this endeavor.

5.3 Solutions

Proposed is a possible solution based on the research of this thesis.

5.3.1 Process

A week-long cybersecurity training for teachers should be held by the USBE with their dedicated team of curriculum and cybersecurity experts (which will now be called the Cybersecurity Team or CT). As this endeavor may take a number of years to develop, it is essential for this team to be created as soon as possible. Their productions will include the making of cybersecurity teaching resources, focused course curriculum, integration in current computing courses, technical teacher training, and updates on curriculum (since new developments appear quite frequently within the field).

The initial meeting should be conducted as an information session with an introduction to the CT and what teachers can expect. The CT will be in charge of conducting the training and the following monthly ones. Such instruction must be based on approved USBE standards and certifications.

5.3.2 Measurements

A survey will be given at the beginning and end of each meeting that includes the same aspects as the one used in this thesis (Appendix A: Qualtrics Survey) and the improvements listed in Section 5.2.3. The background however, can be filled out just once, stored, and then assigned an identification number for each teacher. Overall, this survey will be a measurement on how well the training is being received – whether the teachers see it as beneficial and easy to understand.

When a teacher uses a lesson, plan created by the CT, a test should be given to that teacher's class that same week. The teacher should then fill out a survey for lesson plans. This survey will ask the number of students in the class, the score of each student, the average score, and any additional comments or feedback by the teacher. This should be done each year in the hopes of understanding the impact of each lesson plan and the efficacy of the trainings.

The impact will be measured by student assessment improvement, teacher assessment improvement, number of cybersecurity-focused course offerings, surveys, and number of students participating in these courses. The research part should be done for a minimum of 3-5 years with improvements made to CT's products each year according to results. The results of one year should be compared with those of the previous year to see if the current practices are more or less beneficial and then corrected accordingly.

As the creation and maintenance of the CT and its program will require a large amount of money and time, the timeline and research amount may need to be altered.

REFERENCES

[1] D. McCandless, T. Evans, P. Barton, and S. Tomasevic, "World's Biggest Data Breaches & Hacks | Information is Beautiful," *25th Mars*, 2016. [Online]. Available: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. [Accessed: 06-Jun-2019].

[2] L. Ponemon, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," *Secur. Intell.*, 2018.

[3] Ponemon Institute LLC, "2018 Cost of a Data Breach Study: Global Overview," 2018.

[4] National Initiative for Cybersecurity Careers and Studies, "Glossary | National Initiative for Cybersecurity Careers and Studies," *November 28*, 2018. [Online]. Available: https://niccs.us-cert.gov/about-niccs/glossary. [Accessed: 14-Jun-2019].

[5] Y. K. Peker, L. Ray, and S. da Silva, "Online cybersecurity awareness modules for college and high school students," 2018.

[6] B. of L. S. U.S. Department of Labor, "Occupational Outlook Handbook,Information Security Analysts." [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. [Accessed: 07-Jun-2019].

[7] Steve Morgan, "Cybersecurity Jobs Report 2017 Edition A Special Report from the Editors at Cybersecurity Ventures," 2017.

[8] ISACA and Cybersecurity Nexus, “2016 Cybersecurity Skills Gap,” 2016.

[9] I. L. Chen and L. Shen, “The Cyberethics, Cybersafety, and Cybersecurity at Schools,” 2016.

[10] G. B. White, D. Williams, and K. Harrison, “The CyberPatriot national high school cyber defense competition,” *IEEE Secur. Priv.*, 2010.

[11] T. Ladabouche and S. LaFountain, “GenCyber: Inspiring the Next Generation of Cyber Stars,” *IEEE Secur. Priv.*, 2016.

[12] M. Bashir, C. Wee, N. Memon, and B. Guo, “Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool,” 2017. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2016.10.007. [Accessed: 12-Jun-2018].

[13] J. A. Rursch, A. Luse, and D. Jacobson, “IT-adventures: A program to spark IT interest in high school students using inquiry-based learning with cyber defense, game design, and robotics,” *IEEE Trans. Educ.*, vol. 53, no. 1, pp. 71–79, 2010.

[14] R. S. Cheung and H. Z. Lo, “Challenge Based Learning in Cybersecurity Education.”

[15] J. A. Rursch, A. Luse, and D. Jacobson, “IT-adventures: A program to spark IT interest in high school students using inquiry-based learning with cyber defense, game design, and robotics,” 2018.

[16] NICERC, “Professional Development | NICERC,” *NICERC*, 2016. [Online]. Available: https://nicerc.org/pd/. [Accessed: 28-Jun-2019].

[17] P. Pusey and W. A. Sadera, “Cyberethics, Cybersafety, and Cybersecurity,” 2014.

[18] A. Podhradsky, L. J. LeBlanc, and M. R. Bartolacci, “Personal Denial of Service Attacks (PDOS) and Online Misbehavior: The Need for Cyber Ethics and Information Security Education on University Campuses,” 2014.

[19] National Initiative for Cybersecurity Careers and Studies, “NICE Cybersecurity Workforce Framework | National Initiative for Cybersecurity Careers and Studies,” *National Institute of Standards and Technology*, 2019. [Online]. Available: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework. [Accessed: 20-Mar-2019].

[20] The White House President Barack Obama, “The Comprehensive National Cybersecurity Initiative | The White House,” *the White House President Barack Obama*, 2010. [Online]. Available: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative. [Accessed: 23-Apr-2019].

[21] The White House President Donald Trump, “National Cyber Strategy of the United States of America,” Washington, DC, 2018.

[22] R. Hartley, D. Medlin, and Z. Houlik, “Ethical Hacking: Educating Future Cybersecurity Professionals,” 2017. [Online]. Available: http://iscap.info. [Accessed: 12-Jun-2018].

[23] CyberSeek, “Cybersecurity Supply And Demand Heat Map,” *CyberSeek*. [Online]. Available: https://www.cyberseek.org/heatmap.html. [Accessed: 07-Jun-2019].

[24] M. Anderson and J. Jiang, “Teens, Social Media & Technology 2018,” 2018.

[25] Pew Research Center, “Demographics of Internet and Home Broadband Usage in the United States,” 2019.

[26] C. Cornel, C. Cornel, D. Rowe, S. Moses, “A Cybersecurity Camp for Girls,” *Am. Soc.*

Eng. Educ., no. 123rd, 2016.

[27] R. H. Stalvey, C. Farkas, and C. Eastman, "First use: Introducing information security in high school oracle academy courses," in *Proceedings of the 2012 IEEE 13th International Conference on Information Reuse and Integration, IRI 2012*, 2012.

[28] P. Pape and J. A. Hamilton Jr., "Generating Interest in Cybersecurity Through High School Digital Forensics Education," 2018.

[29] J. Idziorek, J. Rursch, and D. Jacobson, "Security across the curriculum and beyond," 2012.

[30] C. Chou and H. Peng, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience," 2011. [Online]. Available: http://dx.doi.org/10.1016/j.iheduc.2010.03.006. [Accessed: 12-Jun-2018].

[31] G. B. White, D. Williams, and K. Harrison, "The CyberPatriot national high school cyber defense competition," *IEEE Secur. Priv.*, vol. 8, no. 5, pp. 59–61, Sep. 2010.

[32] Y. K. Peker, L. Ray, and S. Da Silva, "Online cybersecurity awareness modules for college and high school students," in *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, 2018, pp. 24–33.

[33] A. Nolan and T. Molla, "Teacher confidence and professional capital," *Teach. Teach. Educ.*, vol. 62, pp. 10–18, Feb. 2017.

[34] L. V. Mangold, "An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs," 2016.

[35] International Technology Education Association and Technology for All Americans

Project, *Standards for Technological Literacy: Content for the Study of Technology*, 3rd ed. Reston, VA: International Technology Education Association, 2007.

[36] National Initiative for Cybersecurity Education and N. I. of S. and T. U.S. Department of Commerce, "Cybersecurity Workforce Demand."

[37] The Utah State Board of Education, "CTE IT Course Information." [Online]. Available: https://www.schools.utah.gov/cte/it/courses. [Accessed: 23-Apr-2019].

[38] J. L. Smith, "Top Ten Cybersecurity Certifications for 2019 - Hack Ware News," *hackerwarenews.com*, 2019. [Online]. Available: https://hackwarenews.com/top-ten-cybersecurity-certifications-for-2019/. [Accessed: 06-Jun-2019].

[39] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," *Comput. Secur.*, vol. 65, pp. 153–165, Mar. 2017.

[40] District or Local Education Agency (LEA) in the Comprehensive Administration of Credentials for Teachers in Utah Schools (CACTUS) system, "Utah Schools Directory," *Utah State Board of Education*, 2017. [Online]. Available: https://www.schools.utah.gov/schoolsdirectory. [Accessed: 31-May-2019].

[41] SurveyMonkey, "Sample Size Calculator: Understanding Sample Sizes | SurveyMonkey," *SurveyMonkey*, 2019. [Online]. Available: https://www.surveymonkey.com/mp/sample-size-calculator/. [Accessed: 03-Jun-2019].

[42] D. Pruitt-Mentle, "State of K12 Cyberethics, Safety and Security Curriculum in U.S.: 2010 Educator Opinion," 2010. [Online]. Available: https://bit.ly/1evqqhd. [Accessed: 12-Jun-2018].

APPENDIX A: QUALTRICS SURVEY – CYBERSECURITY TEACHER PRIMER

Start of Block: Informed Consent

Page Break

Hello!

This research is being conducted under the supervision of Professor Dale Rowe, from the Cybersecurity Research Laboratory.
You are being invited to participate in a research study, "Priming High School Teachers to Instruct Cybersecurity". The goal is to find out why there are few high school teachers that teach cybersecurity courses and what can help increase this.

Your participation in this study will require the completion of the attached questionnaire. This should take approximately 15-20 minutes of your time. Your participation will be anonymous and you will not be contacted again in the future unless you provide contact information (as indicated in one of the questions of the survey). You will not be paid for being in this study. This survey involves minimal risk to you. The benefits, however, may impact society by helping increase the availability of high school cybersecurity courses and providing the needed resources to facilitate this goal.

You do not have to be in this study if you do not want to be. You do not have to answer any question that you do not want to answer for any reason. We will be happy to answer any questions you have about this study. If you have further questions about this project or if you have a research-related problem you may contact me, Cj Cornel at cj.cornel@byu.edu or my advisor, Professor Dale Rowe at dale_rowe@byu.edu
If you have any questions about your rights as a research participant you may contact the IRB Administrator at A-285 ASB, Brigham Young University, Provo, UT 84602; irb@byu.edu; (801) 422-1461. The IRB is a group of people who review research studies to protect the rights and welfare of research participants.

The completion of this survey implies your consent to participate. If you choose to participate, please complete the attached survey by Tuesday, April 30, 2019. Thank you!

End of Block: Informed Consent

Start of Block: Cybersecurity Course Offer

Q1 Do you currently teach, or have taught, at least one high school cybersecurity course within the last year?

- ○ Yes (1)
- ○ No (2)

Page Break

End of Block: Cybersecurity Course Offer

Start of Block: General Questions

Display This Question:

If Q1 = Yes

*

Q2 What cyber certifications do you hold or have held? Please select all that apply.

- ☐ Networking + (1)
- ☐ Cybersecurity + (2)
- ☐ CISSP (3)
- ☐ CEH (4)
- ☐ None (5)
- ☐ Other (6) _____

Display This Question:

If Q1 = Yes

*

Q3 What encourages you to teach (a) cybersecurity course(s)?

_____

_____

_____

_____

_____

Display This Question:

If Q1 = No

Q4 Do you currently implement or have implemented cybersecurity principles in your curriculum within the last year?

- ○ Yes (1)
- ○ No (3)
- ○ Don't know (4)

Display This Question:

If Q4 = Yes

Or Q4 = Don't know

Q5 What cybersecurity principles do you currently include, or have previously included, in your curriculum? Please select all that apply.

- ☐ Password Cybersecurity (1)
- ☐ Online Safety (2)
- ☐ Firewalls (3)
- ☐ Antivirus (4)
- ☐ Networking (5)
- ☐ Forensics (6)
- ☐ Other (7) _____

*

Q6 What barriers do you think are blocking high school technology teachers from implementing cybersecurity principles in their courses? Please select all that apply.

- [ ] Wages (1)
- [ ] Class size (2)
- [ ] School/Institution does not offer enough support (3)
- [ ] Lack of cybersecurity teaching resources (4)
- [ ] Teachers' lack of interest (5)
- [ ] Students' lack of interest (6)
- [ ] Lack of funds (7)
- [ ] There are no barriers (8)
- [ ] Other (9) _____

Q7 What do you think would encourage high school technology teachers to implement cybersecurity principles across the curriculum? Please select all that apply.

- [ ] Pay raise (1)
- [ ] School/institution support (2)
- [ ] Cybersecurity teaching resources (3)
- [ ] Sufficient funds (4)
- [ ] Teacher Training (5)
- [ ] Other (6) _____

Q8 What cybersecurity resources, provided by the Utah State Board of Education, do you currently use? Please check all resources you have used.

- [ ] Teacher Training (1)
- [ ] Class lesson plans (2)
- [ ] List of Cybersecurity Standards (3)
- [ ] None of the above (4)
- [ ] I don't know (5)

Q9 What cybersecurity resources, provided by third parties (e.g. CodeAcademy, CyberPatriot, etc.), do you currently use? Please check all resource types you have used.

- [ ] Teacher Training (1)
- [ ] Class lesson plans (2)
- [ ] List of Cybersecurity Standards (3)
- [ ] None of the above (5)
- [ ] I don't know (6)

Display This Question:

If Q9 = Teacher Training

Or Q9 = List of Cybersecurity Standards

Or Q9 = Class lesson plans

Q10 What third parties do you currently use? Please select all that apply.

- ☐ CyberPatriot (1)
- ☐ cybrary (2)
- ☐ CodeHS (3)
- ☐ TechLearning (4)
- ☐ Pluralsight (5)
- ☐ Other (6) _____

End of Block: General Questions

Start of Block: Cybersecurity Awareness - Confidence

Q11 In general, how confident are you about your ability to teach cybersecurity/information assurance topics?

- ○ Confident (20)
- ○ Somewhat confident (21)
- ○ Neither confident nor unconfident (22)
- ○ Somewhat unconfident (23)
- ○ Not confident (24)

Q12 In general, how comfortable are you with your level of knowledge to teach cybersecurity/information assurance topics?

- Confident (20)
- Somewhat confident (21)
- Neither confident nor unconfident (22)
- Somewhat unconfident (23)
- Not confident (24)

End of Block: Cybersecurity Awareness - Confidence

Start of Block: Cyber Awareness Level - How Likely?

Q13 How aware are you of the cybersecurity implications of *https:* versus *http:* in a website address?

- Aware (1)
- Somewhat aware (2)
- Neither aware nor unaware (3)
- Somewhat unaware (4)
- Unaware (5)

Q14 With your current mobile device, how confident are you in your ability to disable geolocation information from posting to social media?

- Confident (1)
- Somewhat Confident (2)
- Neither confident nor unconfident (3)
- Somewhat unconfident (4)
- Unconfident (5)

Q15 How likely are you to change the default password on an electronic device (e.g. cybersecurity cameras, routers, etc.) that you use?

- Likely (18)
- Somewhat likely (19)
- Neither likely nor unlikely (20)
- Somewhat unlikely (21)
- Unlikely (22)

Q16 How likely are you to connect to an open Wifi?

- Likely (18)
- Somewhat likely (19)
- Neither likely nor unlikely (20)
- Somewhat unlikely (21)
- Unlikely (22)

End of Block: Cyber Awareness Level - How Likely?

Start of Block: Cybersecurity Awareness - Knowledge questions

Q17 What are the three components of information cybersecurity?

- Confidentiality, Integrity, and Availability (1)
- Confidentiality, Internal cybersecurity, and Assurance (2)
- Information Assurance, Non-Repudiation, and Confidentiality (3)
- Logging, Information Cybersecurity, and Monitoring (4)
- I don't know (5)

Q18 What is the best-practice standard for secure web application development?

- OWASP Top-10 (1)
- SQL Injection (2)
- Cross Site Scripting (3)
- Documentation Standards (4)
- I don't know (5)

Q19 Why is patching important?

- ○ Patching is necessary to keep computers operational and online (1)
- ○ Patching is not necessary to securely operate any computer systems. (2)
- ○ Patching reveals critical cybersecurity flaws for the cybersecurity analyst to firewall (3)
- ○ Patching helps keep systems updated and protected against known issues (4)
- ○ I don't know (5)

End of Block: Cybersecurity Awareness - Knowledge questions

Start of Block: The End

Q20 Is there anything else you would like to add?

- ○ Yes (1)
- ○ No (2)

Display This Question:
If Q20 = Yes

Q21 Please put anything you'd like to add.

_____

_____

_____

_____

_____

Q22 In the case that further clarification is needed, would you be willing to discuss this further?

- ○ Yes (1)
- ○ No (2)

Display This Question:

If Q22 = Yes

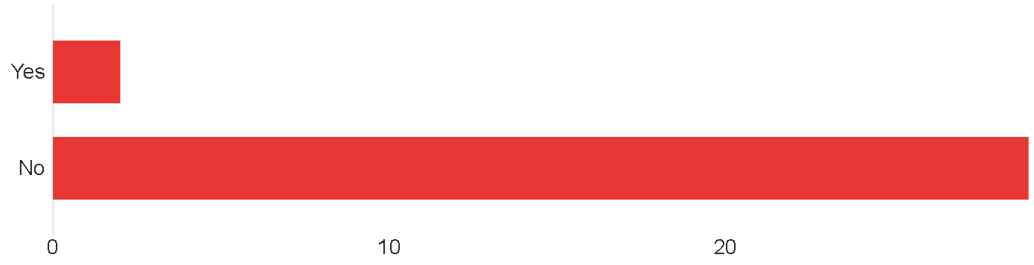
Q23 Please enter your email address.

_____

End of Block: The End

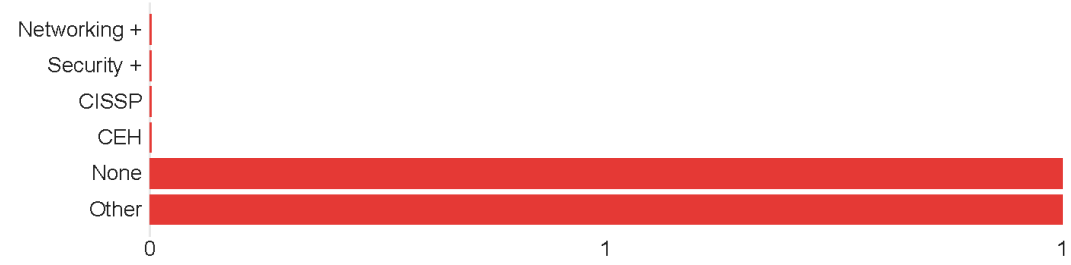
APPENDIX B: SURVEY ANSWERS

Q1 - Do you currently teach, or have taught, at least one high school cybersecurity course within the last year?



Field	Choice Count
Yes	2
No	29
Total	31

Q2 - What cyber certifications do you hold or have held? Please select all that apply.



Field	Choice Count
Networking +	0
Security +	0
CISSP	0
CEH	0
None	1
Other	1
Total	2

Other - Text
Oracle DBA

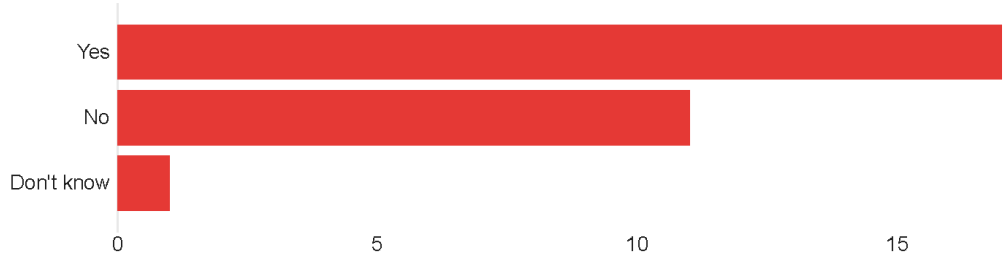
Q3 - What encourages you to teach (a) cybersecurity cours(es)?

What encourages you to teach (a) cybersecurity cours(es)?

It's fun and applicable

Worked for the government to begin with and was the security programmer in my group.

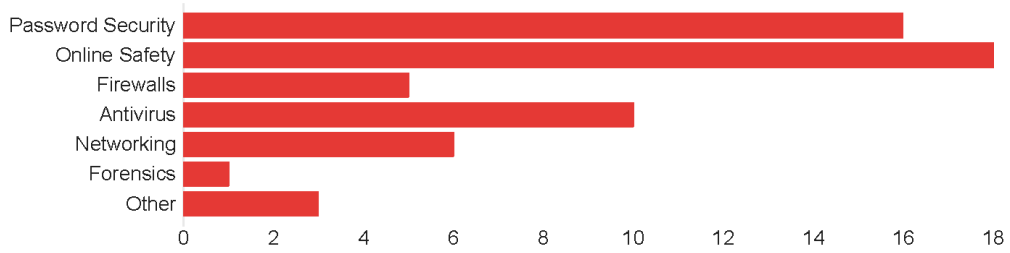
Q4 - Do you currently implement or have implemented cybersecurity principles in your curriculum within the last year?



Field	Min	Max	Mean	Standard Deviation	Variance	Responses
Do you currently implement or have implemented cybersecurity principles in your curriculum within the last year?	1	4	2	1	1	29

Field	Choice Count
Yes	17
No	11
Don't know	1
Total	29

Q5 - What security principles do you currently include, or have previously included, in your curriculum? Please select all that apply.



Field	Choice Count
Password Security	16
Online Safety	18
Firewalls	5
Antivirus	10
Networking	6
Forensics	1
Other	3
Total	59

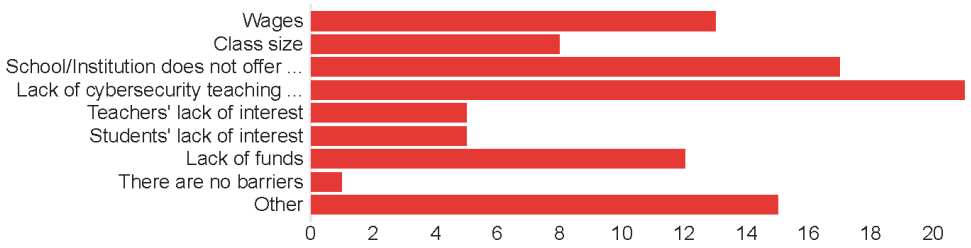
Other - Text

I facilitate the Bridgerland Technical College IT STEM at my high school. There is a course in their program that my students do with includes many of the above. It is a new course this year and so far only have 6 students doing or done with it.

not using real names online

Social engineering, encryption

Q6 - What barriers do you think are blocking high school technology teachers from implementing cybersecurity principles in their courses? Please select all that apply.



Field	Choice Count
Wages	13
Class size	8
School/Institution does not offer enough support	17
Lack of cybersecurity teaching resources	21
Teachers' lack of interest	5
Students' lack of interest	5
Lack of funds	12
There are no barriers	1
Other	15
Total	97

Other - Text
Teacher training
It is not in the core for any courses.

No one is trained. Our computer programming and web development programs are not big yet. Once those are bigger I imagine cyber security would start to be in demand.

N/A

No teacher that is qualified and perhaps a lack of enough students to fill a section.

The district will not offer more types of computer courses when there are other options (i.e. web development, programming, gaming fundamentals, etc.) which are not full.

Course Offerings

We used to offer cybersecurity classes, but a student stole a bunch of software and sold it online and got punished by the federal government. So that added to my lack of interest. I don't think it is a good idea to give students access to anything important.

Time...adding one more thing to a curriculum already over-stuffed with state-mandated performance objectives.

It's not in the strands and standards for the courses I teach.

Time involved in preparing to teach another class when I'm already teaching 5 different IT courses.

At my school we have no barriers around IT classes, just finding class slots for all the different classes.

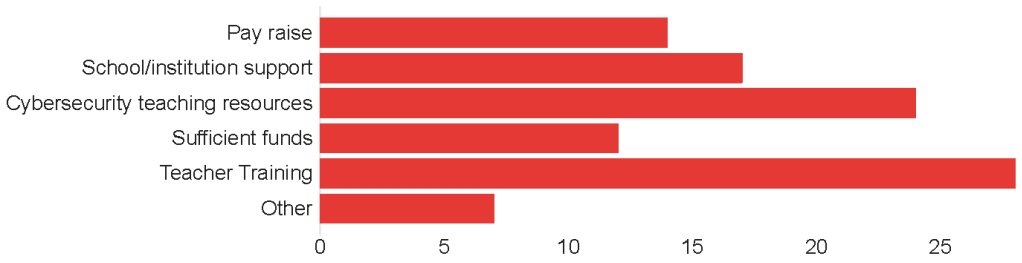
Generally without state level approved courses and strands-standards we are not allowed to teach items not approved at state level.

Teacher knowledge. I don't know wtf I am doing

Need more teacher trainings on it.

Too high a barrier to entry for regular teachers. You might train a run-of-the-mill teacher to do web development or light programming, but for cyber, you need to pull people from industry. And nobody wants to take that pay cut.

Q7 - What do you think would encourage high school technology teachers to implement security principles across the curriculum? Please select all that apply.



Field	Choice Count
Pay raise	14
School/institution support	17
Cybersecurity teaching resources	24
Sufficient funds	12
Teacher Training	28
Other	7
Total	102

Other - Text

The curriculum would need to be updated to include cybersecurity.

I am sure pay is important in that anyone that knows much about cyber security would be out making a WHOLE LOT more doing it than teaching it. Teacher training would require funds.

over-haul performance objectives (highly unlikely)

If It were in the strands and standards of any course I taught, I would include it.

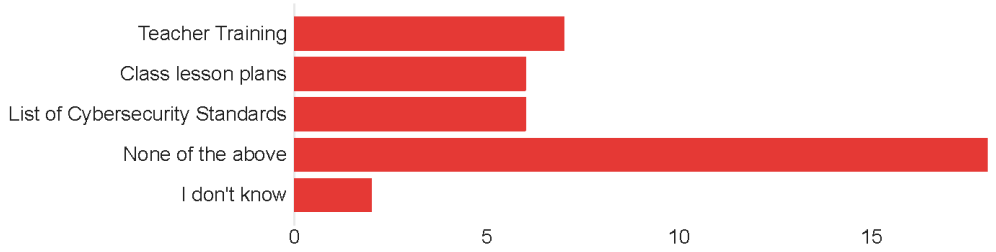
It's not in the strands and standards for the courses I teach.

See answer to previous question.

District admin & IT department support, they are hesitant for students to learn these skills because they are afraid students will then hack their network

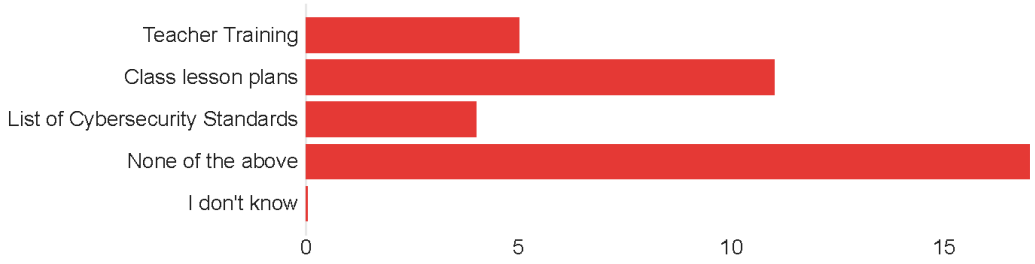
Student interest

Q8 - What cybersecurity resources, provided by the Utah State Board of Education, do you currently use? Please check all resources you have used.



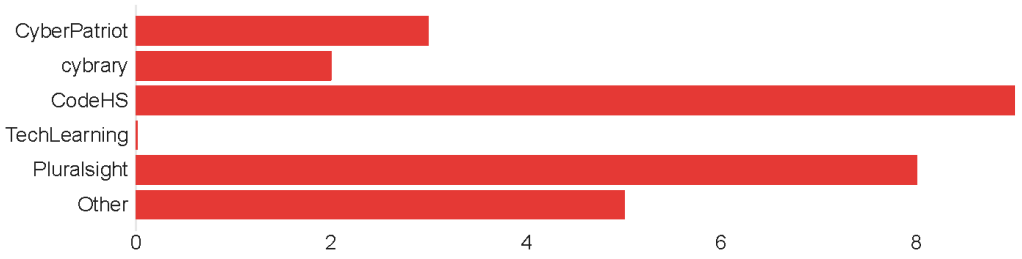
Field	Choice Count
Teacher Training	7
Class lesson plans	6
List of Cybersecurity Standards	6
None of the above	18
I don't know	2
Total	39

Q9 - What cybersecurity resources, provided by third parties (e.g. CodeAcademy, CyberPatriot, etc.), do you currently use? Please check all resource types you have used.



Field	Choice Count
Teacher Training	5
Class lesson plans	11
List of Cybersecurity Standards	4
None of the above	17
I don't know	0
Total	37

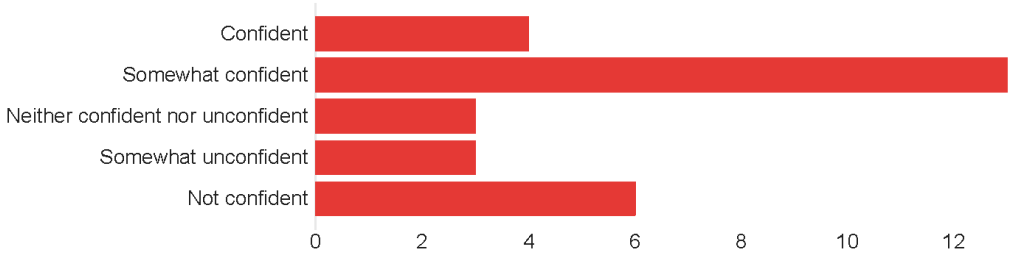
Q10 - What third parties do you currently use? Please select all that apply.



Field	Choice Count
CyberPatriot	3
cybrary	2
CodeHS	9
TechLearning	0
Pluralsight	8
Other	5
Total	27

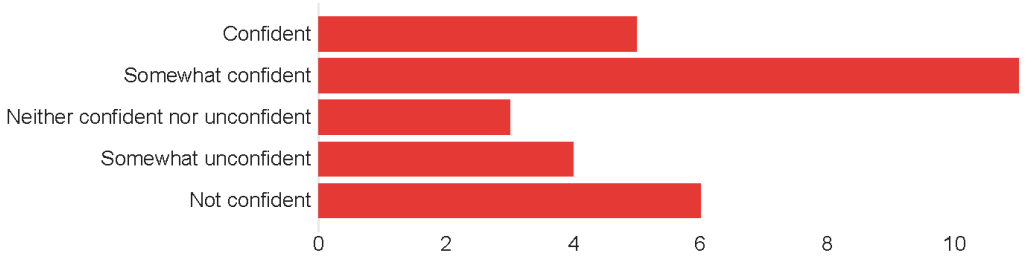
Other - Text
Bridgerland Technical College
Code.org
Industry resources from my 20 years working in IT before becoming a teacher.
Free resources I have obtained at various conferences
Testout

Q11 - In general, how confident are you about your ability to teach cybersecurity/information assurance topics?



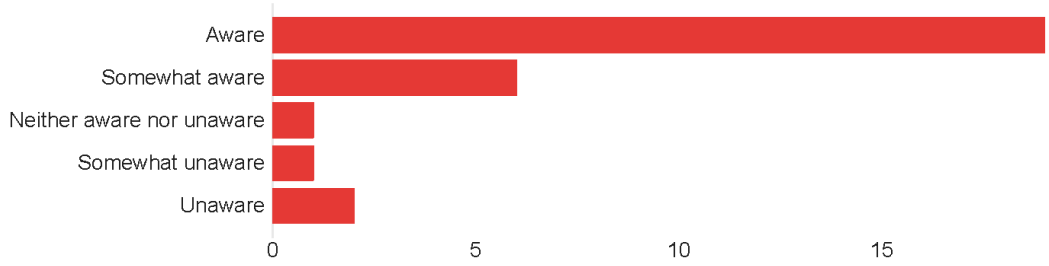
Field	Choice Count
Confident	4
Somewhat confident	13
Neither confident nor unconfident	3
Somewhat unconfident	3
Not confident	6
Total	29

Q12 - In general, how comfortable are you with your level of knowledge to teach cybersecurity/information assurance topics?



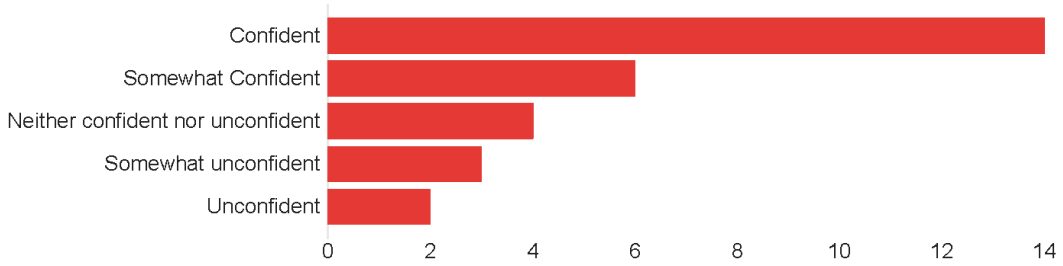
Field	Choice Count
Confident	5
Somewhat confident	11
Neither confident nor unconfident	3
Somewhat unconfident	4
Not confident	6
Total	29

Q13 - How aware are you of the security implications of https: versus http: in a website address?



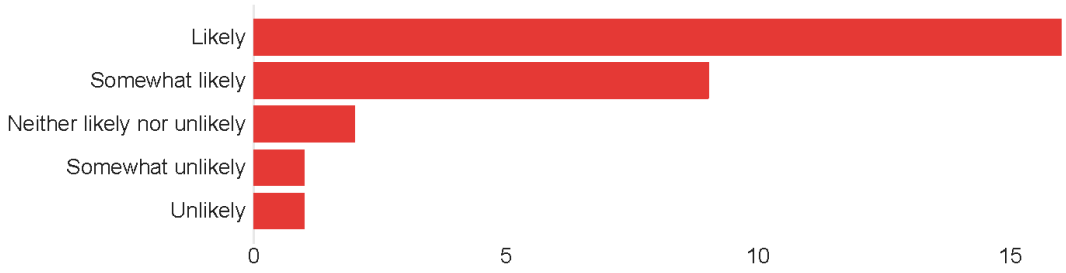
Field	Choice Count
Aware	19
Somewhat aware	6
Neither aware nor unaware	1
Somewhat unaware	1
Unaware	2
Total	29

Q14 - With your current mobile device, how confident are you in your ability to disable geolocation information from posting to social media?



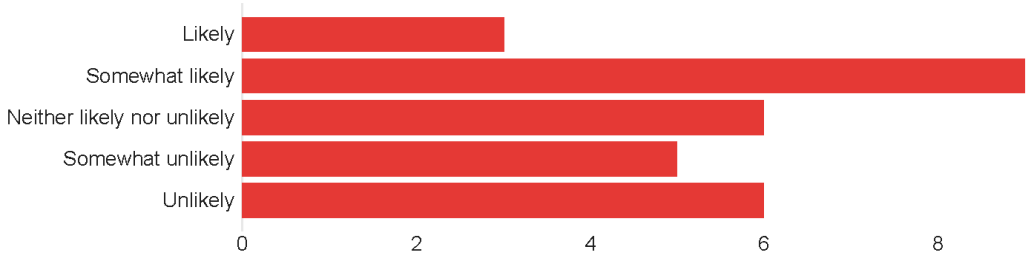
Field	Choice Count
Confident	14
Somewhat Confident	6
Neither confident nor unconfident	4
Somewhat unconfident	3
Unconfident	2
Total	29

Q15 - How likely are you to change the default password on an electronic device (e.g. security cameras, routers, etc.) that you use?



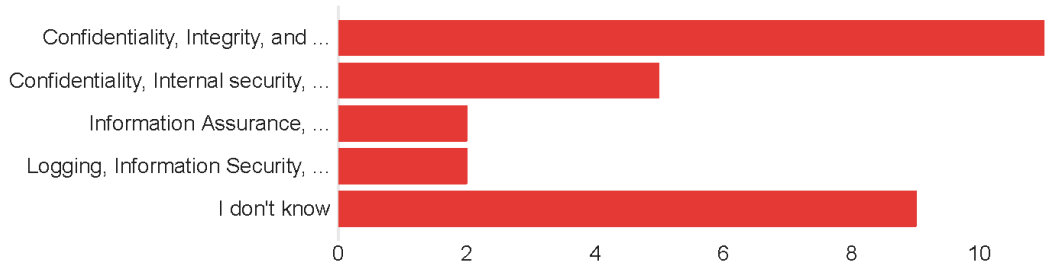
Field	Choice Count
Likely	16
Somewhat likely	9
Neither likely nor unlikely	2
Somewhat unlikely	1
Unlikely	1
Total	29

Q16 - How likely are you to connect to an open Wifi?



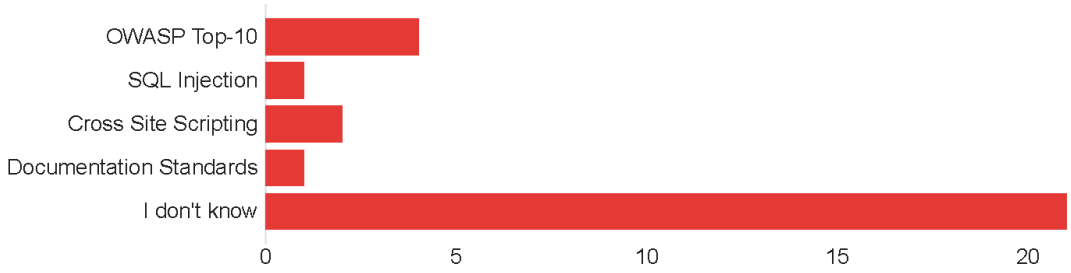
Field	Choice Count
Likely	3
Somewhat likely	9
Neither likely nor unlikely	6
Somewhat unlikely	5
Unlikely	6
Total	29

Q17 - What are the three components of information security?



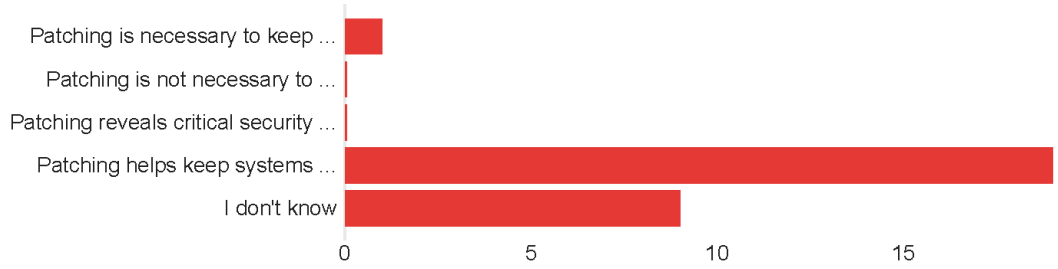
Field	Choice Count
Confidentiality, Integrity, and Availability	11
Confidentiality, Internal security, and Assurance	5
Information Assurance, Non-Repudiation, and Confidentiality	2
Logging, Information Security, and Monitoring	2
I don't know	9
Total	29

Q18 - What is the best-practice standard for secure web application development?



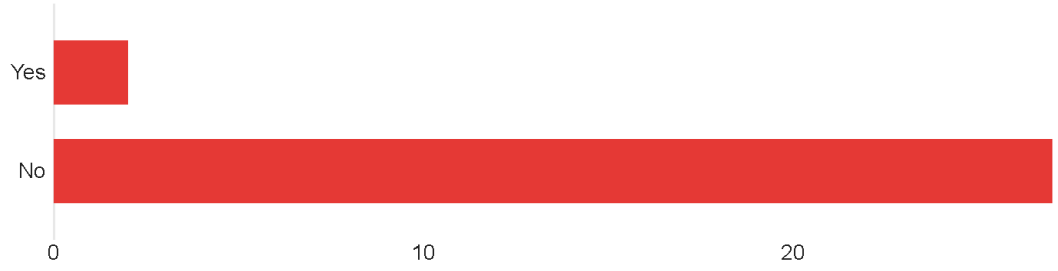
Field	Choice Count
OWASP Top-10	4
SQL Injection	1
Cross Site Scripting	2
Documentation Standards	1
I don't know	21
Total	29

Q19 - Why is patching important?



Field	Choice Count
Patching is necessary to keep computers operational and online	1
Patching is not necessary to securely operate any computer systems.	0
Patching reveals critical security flaws for the security analyst to firewall	0
Patching helps keep systems updated and protected against known issues	19
I don't know	9
Total	29

Q20 - Is there anything else you would like to add?



Field	Choice Count
Yes	2
No	27
Total	29

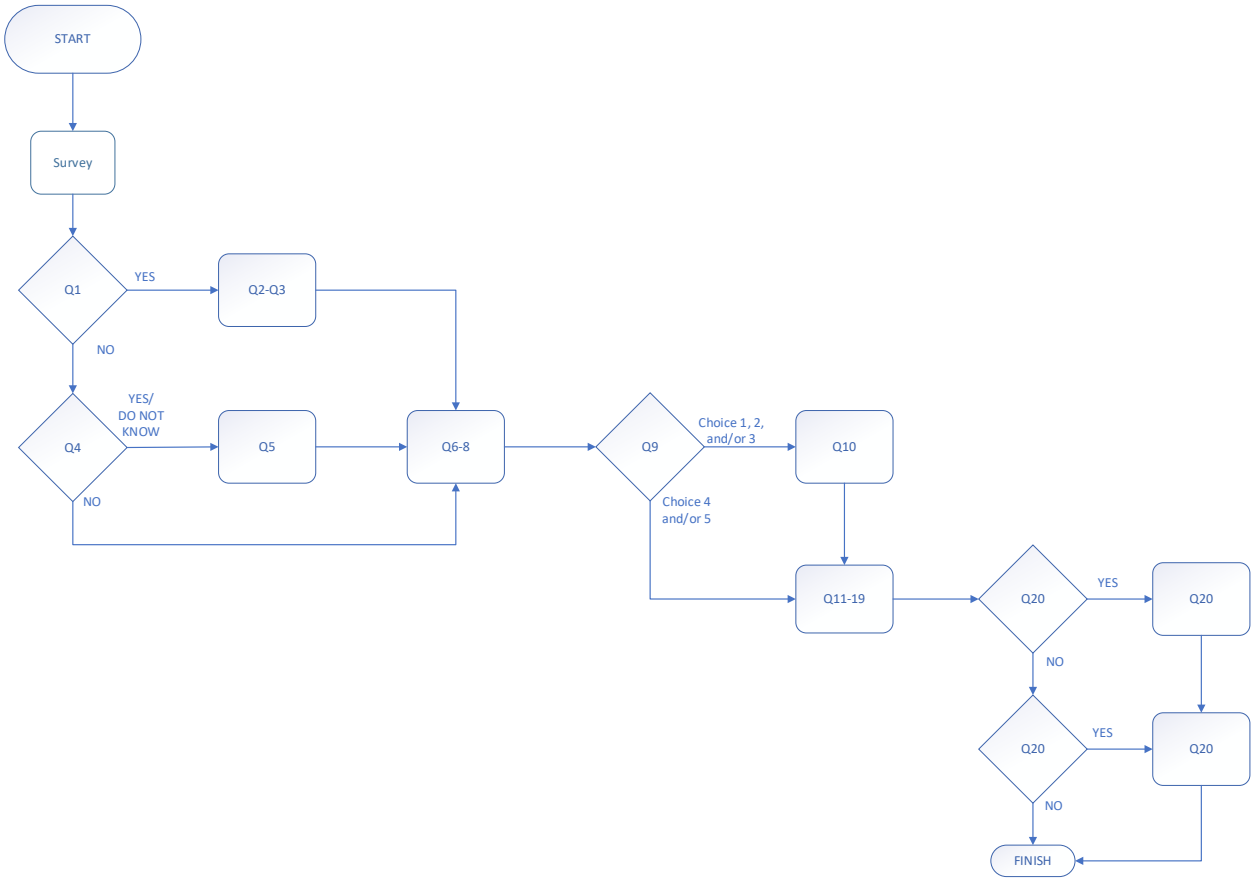
Q21 - Please put anything you'd like to add.

Please put anything you'd like to add.

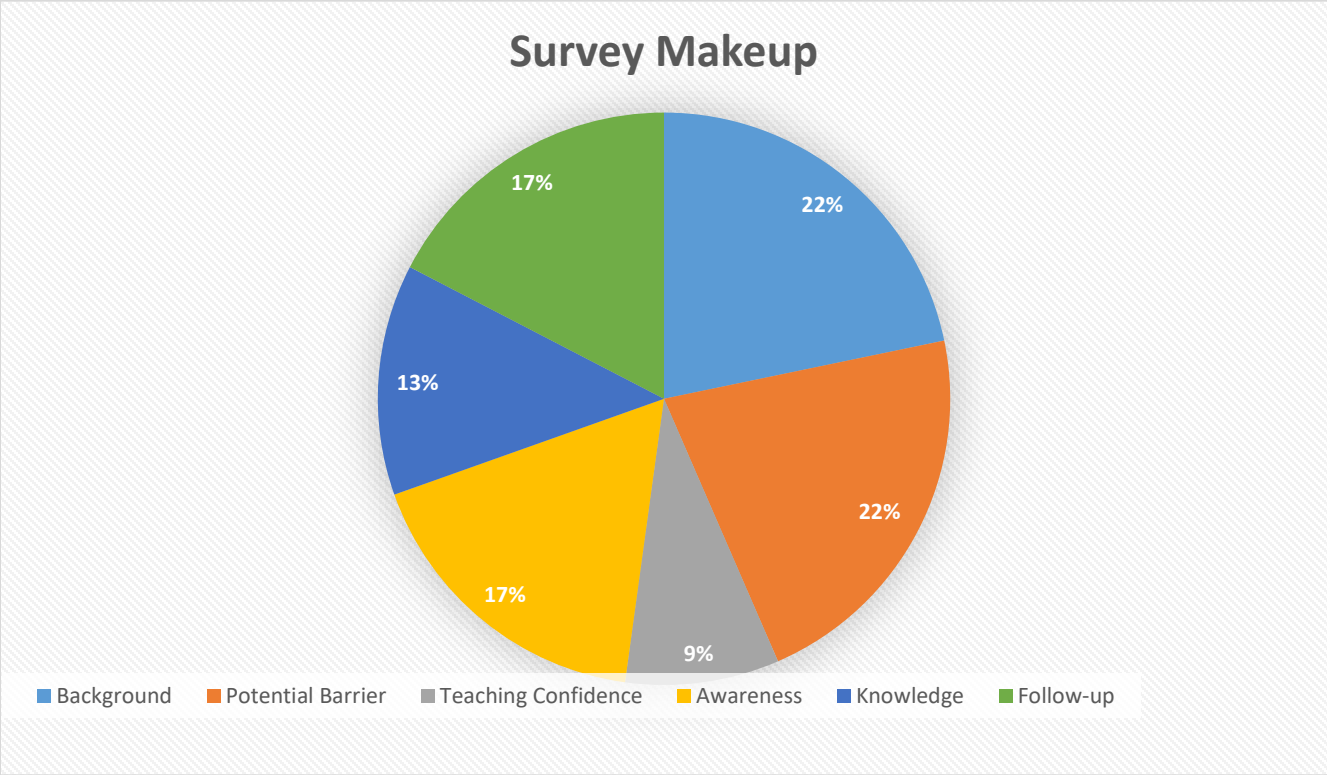
Why is this important? In past 5 years my information has been leaked by Utah state, major hotel chain, major restaurant chain (twice) and a credit bureau.

Cybersecurity has always been a mystery. The USBE trainings I've attended at summer conerence (usually the LDS Business College guy) are generic with no actual practice / application time. I'd like to learn the general principles AND the most common software used. Thank you!

APPENDIX C: QUALTRICS SURVEY QUESTION MAPPING



APPENDIX D: SURVEY TOPIC MAKEUP



APPENDIX E: USBE SECURITY RELATED COURSES

Course	Location on Document	Based on Certification	Certification Base	Security Focused (3 or more security standards)	Security Prerequisite	Prerequisite Course
A+ Computer Maintanence and Repair (11-12) - 35.01.00.00.040	Security (Strand 6, Domain 7.0)	Yes	CompTIA Certification	No	No	Suggested Intro to IT, or Teacher Approval
CISCO Certified Networking Associate, CCNA (10-12) - 35.01.00.00.010	Inaccessible. Based on professional cert, (6.0 Infrastructure Security)	Yes	Cisco Certified Network Associate (200-125)	No	Unknown	-
Computer Programming 1 (10-12) 35.02.00.00.030	Strand 5: Standard 1	No	No	No	No	Suggested - Digital Literacy, Computer Science Principles, or Teacher Approval
Computer Programming 2 (10-12) - 35.02.00.00.040	Strand 5: Standard 1	No	No	No	No	Computer Programming 1 Suggested - Digital Literacy, Computer Science Principles, or Teacher Approval

Computer Science Principles (9-12) - 35.02.00.00.035	Strand 3: Standard 3, Strand 6: Standard 3		No	No	No	No
Database Development (9-12) - 35.02.00.00.021	Strand 5: Standard 1	No	No	No	No	No
Exploring Computer Science 1 (7-9) - 35.02.00.00.007	Strand 3: Standard 4	No	No	No	No	No
Exploring Computer Science 2 (7-9) - 35.02.00.00.008	Strand 1: Standard 1	No	No	No	No	No
Introduction to Information Technology (9-12) - 35.02.00.00.005	Strand 1: Standard 2, Strand 4: Standards 2 & 9, Strand 7: Standard 2	No	No	Yes	No	No
Linux Fundamentals (11-12) - 35.01.00.00.025	Strand 4: Standard 5	Yes	CompTIA Linux+ [Powered by LPI]	No	No	No
Network Fundamentals (10-12) - 35.01.00.00.030	Domain 5: Network Security	Yes	CompTIA 2011 Network+	Yes	No	No
Security Fundamentals (10-12) - 35.01.00.00.036	Network security, communication security, infrastructure security…	Yes	MTA Security Fundamentals and CompTIA Security+ IT Industry certs	Yes	No	No
Web Development Capstone (10-12) - 35..0.00.00.067	Strand 1: Standard 2, Strand 2: Standard 5 (MongoDB	No	No	No	No	No

	Security, Security & Deployment)					

APPENDIX F: SURVEY MAP TO THE NICE FRAMEWORK

Survey Question #	NICE Framework Component
1-4	n/a
5	• Analyze: Threat Analysis • Collect and Operate: Cyber Operations • Investigate: Digital Forensics • Operate and Maintain: Network Services • Oversee and Govern: Training, Education, and Awareness • Protect & Defend: Vulnerability Assessment and Management • Securely Provision: Risk Management
6-12	n/a
13-15	• Oversee and Govern: Training, Education, and Awareness
16	• Analyze: Exploitation Analysis
17	• Analyze: Exploitation Analysis • Operate and Maintain: Systems Analysis, Systems Administration • Securely Provision: Systems Architecture
18	• Operate and Maintain: Data Administration • Securely Provision: Software Development
19	• Operate and Maintain: Customer Service and Technical Support
20-23	n/a

APPENDIX G: SURVEY ASSESSMENT SOURCES

Source	Assessment	Question	How it Works
Online Cybersecurity Awareness Modules for College and High School Students [5]	Awareness	How likely are you to change the default password on an electronic gadget (for example, a web cam) you use? How aware are you of the cybersecurity implications of *https:* versus *http:* in website addresses? How careful are you when posting your location or photos on social media? How concerned are you about connecting to an open Wi-Fi?	Participants were asked to self-assess their awareness level/concern on a scale of 1-4, 1 being least concern and 4 being the most concern. The test used is called the Cybersecurity Awareness Scores (CAS)
Profiling cybersecurity competition participants: Self-efficacy,	Teaching Confidence	In general, how confident are you about your ability to work in the cybersecurity/ information assurance field?	Scale of 1-7, with 7 representing high efficacy.

decision-making and interests predict effectiveness of competitions as a recruitment tool [12]		In general, how comfortable are you with your level of knowledge to work in cybersecurity/information assurance field?	
An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs [34]	Knowledge	What are the three components of information cybersecurity? Confidentiality, Integrity, and Availability (CIA triad). Why is patching important? Patching helps keep systems updated and protected against known issues. What is the best-practice standard for secure web application development? OWASP Top-10.	Questions were asked with 5 answers given, 1st being correct and 5 being IDK.

APPENDIX H: SCHOOL DISTRICT TEACHER NUMBERS

School District	Computer Teachers	Teachers that taught Cybersecurity-related Course(s)	Teachers that taught Cybersecurity-focused Course(s)
Alpine	22	13	2
Box Elder	-	-	-
Cache County	4	4	1
Canyons	12	9	0
Davis	-	-	-
Granite	4	2	0
Jordan	4	2	0
Logan City	-	-	-
Murray City	1	1	0
Nebo	11	9	1
Salt Lake City	5	4	0
Uintah	-	-	-
Washington County	5	4	1

Total	68	48	7

** Those that have the dash (-) had no data available

APPENDIX I: SURVEY DISTRIBUTION METHODS

Email:

Hello!

I'm currently working on gathering data for my thesis and would love to have you participate.

The goal is of this research is to find out why there are few high school teachers that teach cybersecurity courses and what can help increase this.

https://byu.az1.qualtrics.com/jfe/form/SV_elbV1ZzoaaerlOd

Could you please pass this around to other Utah high school teachers that teach a computer related course?

Many thanks,

Website Link:

https://byu.az1.qualtrics.com/jfe/form/SV_elbV1ZzoaaerlOd

QR Code:

ACRONYMS

BYU – Brigham Young University

C3 - Cyberethics, Cybersafety, and Cybersecurity

CAS - Cybersecurity Awareness Scores test

CEH - Certified Ethical Hacker

CISSP - Certified Information Systems Cybersecurity Professional

CNCI - President George W. Bush's Comprehensive National Cybersecurity Initiative

CompTIA - Information Technology Industry & Association

CT – Cybersecurity Team

CTE – Career and Technical Education

HTTP – Hypertext Transfer Protocol

HTTPS – (Secure) Hypertext Transfer Protocol

$(ISC)^2$ - International Information Systems Cybersecurity Certification Consortium, Inc.

IT – Information Technology

NICE - National Initiative for Cybersecurity Education

USBE – Utah State Board of Education

USD – United States Dollar

DEFINITIONS

Breach - the act of gaining unauthorized access to a restricted space that usually contains sensitive information such as customer or employee personal identifying information.

Computer Course – A course that teaches a computer literacy skill that involves understanding how the commuter works or communicates. Examples of these courses include Computer Tech, Web Development, Tech Literacy, Computer Programming, etc.

Cybersecurity – "activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (3)

Cybersecurity-focused Course – A course that focuses on three or more cybersecurity standards as listed in their Course Strands & Standards or information document

Cybersecurity-related Course – A course that reviewed at least one cybersecurity aspect, or had a cybersecurity prerequisite as listed in their Course Strands & Standards or information document

Cybersecurity Team (CT) – proposed unit of curriculum and cybersecurity experts dedicated to the development of USBE's cybersecurity teacher resources and training.

Inservice Teacher – A teacher that is currently working.

Preservice Teacher – A person learning how to become a certified academic teacher