Brigham Young University
BYU ScholarsArchive

Theses and Dissertations

2019-08-01

Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity

Desiree Marie Winters
Brigham Young University

Follow this and additional works at: https://scholarsarchive.byu.edu/etd

BYU ScholarsArchive Citation
Winters, Desiree Marie, "Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity" (2019). *Theses and Dissertations*. 7558.
https://scholarsarchive.byu.edu/etd/7558

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.

Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity

Desiree Marie Winters

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

Master of Science

Jason K. McDonald, Chair
Derek L. Hansen
Heather M. Leary

Department of Instructional Psychology and Technology

Brigham Young University

Copyright © 2019 Desiree Marie Winters

All Rights Reserved

ABSTRACT

Using Playable Case Studies to Influence Teen Girls' Self-Efficacy and Interest in Cybersecurity

Desiree Marie Winters
Department of Instructional Psychology and Technology, BYU
Master of Science

Various factors dissuade women from the field of cybersecurity. Educational interventions are needed to mitigate the negative effects of stereotypes and low perceived self-efficacy and help girls gain interest in learning about cybersecurity. This thesis focuses on an intervention targeted to increase teenage girls' interest and self-efficacy in cybersecurity: the Cybermatics Playable Case Study. Findings from a mixed-methods study in which a focus group was conducted with 7 middle school girls, interviews were conducted with 2 high school girls, and pre- and post- simulation survey was collected from all 9 participants reveal tensions between enjoyment and frustration in the girls' experience with Cybermatics and their desire for both autonomy in completing tasks and the availability of help when needed. Almost all of the study participants indicated that their experience with the Playable Case Study made them more interested in cybersecurity and feel more confident in their ability to do well in a cybersecurity class, although the quantitative data revealed considerable complexity in the girls' perceptions of these constructs and significant lack of prior knowledge of cybersecurity. Quantitative survey data illustrates correlations between successful completion and enjoyment of the simulation, interest, and self-efficacy. Qualitative data from the focus group and 2 individual interviews shed light on what may be the simulation's greatest benefit: giving exposure to cybersecurity to teen girls in a way that is interesting and provides an accurate portrayal of the work of a security analyst.

Keywords: simulation, computer simulation, cybersecurity, playable case study, self-efficacy

ACKNOWLEDGMENTS

I would like to thank my committee members for their guidance and feedback throughout the process of this study and the writing of this thesis. I am particularly indebted to my advisor, Jason McDonald, who provided support without which this thesis would not have been completed. I would also like to thank Stephen Yanchar for his assistance as a writing consultant in the early stages of this thesis. Finally, I would like to thank Derek Hansen and all the members of the BYU PCS team who helped create Cybermatics, and the teachers and students who were willing to use Cybermatics in their classes for the sake of this research.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

Introduction

While cybersecurity is a rapidly growing field with robust career opportunities, women remain underrepresented in cybersecurity-related careers (Bureau of Labor Statistics, U.S. Department of Labor, 2018; Frost & Sullivan, 2017). A complex combination of external barriers, which prevent women from having successful experiences in the field, and internal deterrents, which cause women to select other courses of study, perpetuate this discrepancy (Cheryan, Master, & Meltzoff, 2015; Cohoon & Aspray, 2006). More women are needed in the field to increase equal opportunity, allow for the inclusion of diverse perspectives, and to help fill the employment gap, which is expected to continue to increase (Cheryan et al., 2015; Kalwarski, Mosher, Paskin, & Rosato, 2007; Margolis & Fisher, 2003).

What has caused this underrepresentation of women in cybersecurity? And how can it be overcome? For one thing, this underrepresentation in professional practice is an extension, and perhaps partially a result, of underrepresentation in educational tracks that lead to computer science-related professions (Cohoon & Aspray, 2006). Research indicates that girls have lower self-efficacy in computer science-related fields (Bagchi-Sen, Rao, Upadhyaya, & Chai, 2010; Cheryan et al., 2015; Jethwani, Memon, Seo, & Richer, 2017), and self-efficacy seems to be an important factor influencing career choice (Hackett, 1995).

While cybersecurity camps and competitions are gaining popularity and seeking to increase student interest in cybersecurity, these current interventions are failing to attract students who do not already have cybersecurity experience. At Brigham Young University, students and faculty in the Information Technology, Creative Writing, and Instructional Psychology and Technology departments have worked together to create a new intervention,

targeted to increasing girls' self-efficacy in cybersecurity and attract students who are not already interested in the field.

This thesis describes the test of this new intervention designed to introduce students with little to no background in cybersecurity to the field. The intervention is a new educational platform called a Playable Case Study (PCS), which incorporates elements of virtual internships and alternate reality games in a computer-based simulation that can be incorporated into classroom curriculum.

Prior to this study, the PCS had been formally tested in university courses, and data collected from Information Technology students' participation in the PCS. This thesis presents the findings of testing the PCS with high school-age students in order to see specifically how the PCS influences girls' self-efficacy in pursuing further education in cybersecurity.

This study aims to address the following research questions:

1. What was the experience of the teen girls who used the PCS?
2. Did the experience with the PCS change the girls' interest in cybersecurity?
3. Did the experience with the PCS change the girls' self-efficacy in their ability to be successful in a cybersecurity class?

CHAPTER 2

Literature Review

In this section, I will outline the need for cybersecurity professionals and the underrepresentation of women in the field. I will then discuss some possible reasons for that underrepresentation, including male-dominant stereotypes of the field and low self-efficacy with tasks relating to computer science. Finally, I will briefly discuss some of the current interventions used to attract students to the field of cybersecurity and the opportunity for a new intervention focused on introducing high school girls to cybersecurity and designed specifically to address some of the issues that may be dissuading women from entering the field of cybersecurity.

The Need for Women in Cybersecurity

Cybersecurity is currently one of the fastest-growing professions in the U.S. (Bureau of Labor Statistics, 2018). With 100,000 employed security analysts in 2016, the job opportunities are anticipated to grow by 28% between 2016 and 2026. It is estimated that by 2022, there will be 1.8 million unfilled positions within the field of cybersecurity (Frost & Sullivan, 2017).

Despite the ever-growing need for cybersecurity professionals, there remains a severe underrepresentation of women in the field. The 2018 report published by the U.S. Department of Labor Statistics indicated that only 20.2% of information security analysts were women. According to a report by the National Science Fountation (NSF), women made up only about 25% of bachelors, masters, and/or doctorate graduates in computer and information scientist professions (National Science Foundation, National Center for Science and Engineering Statistics, 2017).

This underrepresentation of women and minorities poses several problems. First, as cybersecurity is a field with excellent job opportunities, high salaries, and good job security, women should not be excluded from these desirable jobs (Kalwarski et al., 2007). But the gender disparity is more than an issue of fairness and equal opportunity for women; the field needs the unique perspectives and contributions of women (Hill, Corbett, & St. Rose, 2010; Margolis & Fisher, 2003). And perhaps at the most basic level, employing greater numbers of women (and underrepresented groups) in cybersecurity jobs will help fill the workforce gap (Cheryan et al., 2015).

Deterrents and Barriers to Women in Cybersecurity

What is keeping women from jobs in cybersecurity? Although this is a fairly recently-asked question, there is much in the literature of computer science on the factors that dissuade women from computer science careers. That body of literature may help inform the issue of women's underrepresentation in cybersecurity, as cybersecurity is closely related to computer science. The research and discussion on the topic are multifaceted, pointing various interwoven constructs. I will first present briefly some external obstacles that keep women from the field or from experiencing success in computer science and cybersecurity careers, and then discuss internal obstacles, or reasons why women may self-select out of such careers.

External barriers. In response to women's underrepresentation in computer science and cybersecurity fields, are female students supported and encouraged to enter these fields by individuals in mentor and advisory roles? The answer seems to be no. In one study, less than half of the faculty reported that they encouraged students to persist in the computer science program (Cohoon & Aspray, 2006). In fact, it seems to be the case that girls are actually steered away from the cybersecurity and computer science by parents, teachers, counselors, and other

advisors who perceive that the field is “for boys” (Cheryan et al., 2015; Eccles, Jacobs, & Harold, 1990; Sadker, & Sadker, 2010). Cohoon & Aspray, 2006) noted that women experienced a lack of same-gender peer support and the lack of faculty mentoring and encouragement, factors which ultimately contributed to women leaving computer science programs.

This message that cybersecurity is not a field for women seems to extend to the workplace. Wynn and Correll (2018) observed various ways that technology companies alienated women at recruiting events, including excluding women from the presentation and discussion, referencing masculine geek culture, and using and enforcing gender stereotypes in presentation content. Frost & Sullivan (2017) reported that 51% of the female cybersecurity professionals surveyed indicated that they experienced discrimination of some kind. Furthermore, it would appear that women experience unequal opportunities for career advancement in cybersecurity careers, evidenced by the fact that, even controlling for the general underrepresentation of women in the cybersecurity, women are even more disproportionately underrepresented in leadership and executive positions, and women statistically have lower salaries than men (Bagchi-Sen et al., 2010; Cheryan et al., 2015; Frost & Sullivan, 2017). Women in cybersecurity roles also report feeling undervalued (Peacock & Irons, 2017) and seem to be punished for excelling in traditionally male roles (Cheryan et al., 2015). As a result, even women who have succeeded in obtaining a job in cybersecurity may ultimately decide to leave the field.

As stated previously, one of the main reasons why the underrepresentation of women in cybersecurity is considered problematic is that women should not be kept from well-paying and desirable jobs in the field. This is why it is so important these external barriers keeping women

from entering and experiencing success in cybersecurity are understood. However, this argument becomes irrelevant if cybersecurity careers are not, in fact, desirable to women. In the next section, I will discuss some of the internal factors, or reasons that girls and women may choose to steer away from these fields.

Internal deterrents. Oakes (1990) investigated opportunities and retainment of women and minorities in STEM fields and used the term "educational pipeline" to refer to the track of educational experiences "through which all scientific personnel flow," noting the choice that many women and minorities make to leave the pipeline at certain critical junctures. Since Oakes's work, numerous researchers have examined the "leaky pipeline" phenomenon (Blickenstaff, 2005; Hill et al., 2010; Pell, 1996) and have explored possible reasons as to why girls and women may self-select to leave the pipeline, choosing not to pursue computer science careers. This section will discuss some of these reasons, including beliefs that may cause women to not be interested in computer science-related careers, and other factors that impede women's ability to feel capable of success in such careers.

Goals and roles. One reason that women may choose not to pursue programs and careers in computer science-related fields is that women (more so than men, generally speaking) tend to value communal goals and do not anticipate that computer science careers will fulfill those goals (Dampier, Kelly, & Carr, 2012; Jethwani et al., 2017; Shumba et al., 2013). In fact, women may view STEM careers as impeding communal goals (Diekman, Brown, Johnston, & Clark, 2010), and therefore may be deterred from the field by the mismatch between their own goals and their perception of computer science-related careers.

An additional reason why women may feel dissuaded from cybersecurity is that traditional women's roles seem in conflict with a cybersecurity career. The hacker culture

traditionally associated with computer science fields seems at odds with traditional family roles for women, and research suggests that women choose to avoid such careers where they anticipate work/family conflict (Cheryan et al., 2015; Morgan, Gelbgiser, & Weeden, 2013). If women (speaking generally) do not feel that their values are supported by a cybersecurity career, this perceived misfit could contribute to the disproportionally low representation of women in the field (Eccles, 1987).

Effects of stereotypes. While the existence of stereotypes about cybersecurity may be obvious, at this point in the discussion, it seems worthwhile to draw attention to those stereotypes and discuss the impact that they have on women. Traditionally, the prevailing stereotype of computer scientists has been one of a geeky, socially awkward, male, infatuated with computers (Cheryan et al., 2015; Schott & Selwyn, 2000). Margolis and Fisher's (2003) research at Carnegie Mellon, home of one of the nation's top computer science programs, captured the essence of the stereotypes that prevail about computer science-related fields. Students described computer science peers as being "myopically focused" on computers, "living and breathing the world of computing," staring at their screens, gradually developing a "monitor tan" (p. 65). The School of Computer Science (SCS) was colloquially re-named with such acronyms as "See, Can't Socialize," "Sleep, Code, Sleep," and "Socially Challenged Students" (p. 65).

While our culture has become increasingly tech-dependent, with 78% of U.S. homes reporting having a computer in 2015 (Ryan & Lewis, 2017), one might expect that this stereotype would have dissipated over the years. However, more recent studies indicate that these stereotypes are still prevalent in the educational contexts both in the U.S. and abroad (Berg, Sharpe, & Aitkin, 2018; Ehrlinger et al., 2018; Master, Cheryan, & Meltzoff, 2016).

Compared to boys, girls feel less association with these stereotypes, which are perceived as unfeminine. Thom, Pickering, and Thompson (2002), reported that many of the young women he talked to during the eight years of his study were uninterested in a technical career for fear of becoming "de-feminized." Even the presence of stereotype-associated objects in a computer science classroom has been shown to cause female students to feel less sense of belonging in computer science environments (Master et al., 2016). Girls are less likely, compared to boys, to feel they fit the stereotypes, and therefore report less belonging. This sense of misfit mediates less interest in enrolling in computer science courses.

Some women, however, may be interested in computer science, but still driven away by the negative effects that awareness of these stereotypes may have on their ability to excel in the field. This leads us to the phenomenon of stereotype threat, a term introduced by Steele (1997) as:

> a situational threat . . . that, in general form, can affect the members of any group about whom a negative stereotype exists (e.g., skateboarders, older adults, White men, gang members). Where bad stereotypes about these groups apply, members of these groups can fear being reduced to that stereotype. And for those who identify with the domain to which the stereotype is relevant, this predicament can be self-threatening. (p. 614)

For many women, stereotypes inform their perceptions of the field, which do not align with their self-perceptions; they do not feel like they fit the mold of someone who would work in cybersecurity. In some cases, these beliefs are reinforced by men in the field who make harassing comments and draw attention to the fact that they are different from most members of the field, on the basis of their sex (Margolis & Fisher, 2003). Thus, they fall victim to stereotype

threat, “the threat that others' judgments or their own actions will negatively stereotype them in the domain” (Steele, 1997, p. 613).

Stereotype threat is damaging in the effects it has on an individual’s self-evaluative anxiety, and although Steele (1997) distinguishes the construct of self-evaluative anxiety from self-efficacy, he does point to increasing domain self-efficacy as a way to reduce the effects of stereotype threat. Self-efficacy is a construct which has been studied extensively in the context of women in computer science, and, to a lesser degree, women in cybersecurity, and is the next topic of our discussion.

Self-efficacy. An individual’s efficacy expectations, or her conviction that she can successfully execute the behavior required to produce a given outcome, will determine how much effort she will expend on a given task, how long she will persist through adversity, and whether she will initiate coping behavior (Bandura, 1977). Bandura (1977) explained, “Expectations of personal efficacy are derived from: performance accomplishments, vicarious experience, verbal persuasion, and physiological states” (p. 191). Therefore, prior experience (even vicarious experience) and success in a given field or task, encouragement, and even how one is feeling can all contribute to one’s belief that she will be successful in a given task, and, in turn, determine whether she will demonstrate the tenacity and coping behaviors needed to actually be successful.

Numerous studies have demonstrated that girls report lower self-efficacy in computer science-related fields (Bagchi-Sen et al., 2010; Jethwani et al., 2017). Cheryan et al. (2015) point out that one of the reasons that women may choose not to pursue cybersecurity is that they “underestimate how well they will do.”

Bandura, Barbaraneli, Caprara, and Pastorelli (2001) indicated the importance of self-efficacy in enabling people to pursue a goal despite opposition, even in the case of career pursuit: "Among the mechanisms of human agency, none is more focal or pervading than people's perceived self-efficacy. Unless people believe they can produce desired outcomes by their actions, they have little incentive to act or to persevere in the face of difficulties. ... Perceived self-efficacy is, therefore, posited as a pivotal factor in career choice and development" (p. 187). Understanding the role that self-efficacy can play in the choice and pursuit of a career, the fact that women, as compared to men, experience much lower self-efficacy in computer science, and cybersecurity in particular, is of great concern.

In summary, the literature points to a variety of interwoven constructs that contribute to the leaky pipeline and ultimately the underrepresentation of women in cybersecurity. External factors, such as discouragement from mentors and advisors and unequal opportunity in cybersecurity careers may turn women away from the field. Internal factors play a part as well, and women may not feel that their own values align with a cybersecurity career. However, even women who might be interested in a cybersecurity career are at risk of stereotype threat and low self-efficacy. As these factors combine, girls see that cybersecurity is a male-dominated field, one in which they feel they may not have a place, and the underrepresentation perpetuates itself (Cheryan et al., 2015).

The following sections will further examine some of the constructs described by or relating to the internal factors described here and how education generally may help mitigate some of these deterrents and promote more adaptive learning behaviors in challenging contexts.

Education and Combating Stereotypes

Steele (1997) described not only the phenomenon of stereotype threat, but also a strategy for reducing it. Steele called this strategy for reducing the effects of stereotype threat in schools "wise schooling" (p. 625). The recommended strategies are different for students who already identify with the given domain (i.e. women majoring in engineering who identify as engineers) versus those who do not. Specifically, for domain-identified students, Steele suggests affirming domain belongingness, demonstrating the value of multiple perspectives or approaches to the academic substance and culture, and having role models. For domain-unidentified students, Steele suggests non-judgmental responsiveness (or little attention to whether the student's answers are right or wrong) and building self-efficacy. For both groups, however, the following strategies may be used: providing optimistic teacher-student relationships, assigning challenging, rather than remedial, work; and stressing the expandability of intelligence (this concept will be revisited later in this literature review). Steele's work (1997) suggested that these wise school practices could be successful in increasing Black students' performance in the academic environment. These wise school practices have been shown in other research to reduce stereotype threat and have a positive influence on students' academic career aspirations (Taylor & Anthony, 2000).

More generally speaking, attempts at negating the effects of stereotypes have been used in the fields of business and medicine. Exposing students to a curriculum recommended by the Association to Advance Collegiate Schools of Business on the importance of diversity appears to lead to fewer gender stereotypes among business students (Paris & Decker, 2012), and exposing doctors and nurses to educational programs on diminishing stereotypes and fostering positive perceptions and collaboration between the two roles seems to have positive effects on their

working relationship, which is often inhibited by stereotypes of their roles (Carpenter, 1995). Students and professionals in various fields are impacted by the effects of stereotypes and stereotype threat, but the literature gives hope that those negative effects can be negated through various types of educational programs.

Education and Self-Efficacy

The literature on self-efficacy also describes the potential for self-efficacy beliefs to change through treatment. Bandura (1977) described not only four sources of efficacy expectations, but also modes of induction for each. To encourage performance accomplishments, the first source of efficacy expectations described, treatment could include participant modeling, performance desensitization, performance exposure, and self-instructed performance. To encourage the second source of efficacy expectations, vicarious experience, subjects might be exposed to live modeling or symbolic modeling. Verbal persuasion, the third source described by Bandura, may be achieved through suggestion, exhortation, self-instruction, or interpretive treatments. Emotional arousal, the last of Bandura's sources of efficacy expectations, may be affected by attribution, relaxion and biofeedback, symbolic desensitization, and symbolic exposure. Bandura's work indicates that these means of treatment can be successful in promoting behavioral changes through increased self-efficacy.

While Bandura's (1977) initial research dealt largely with individuals overcoming phobias, these findings are supported in broader contexts. Self-efficacy does appear to be an important factor of success in the academic setting, influencing students' willingness to participate, work hard, persist in challenging tasks, and their ability to engage in self-regulated learning and to maintain a positive emotional state (Zimmerman, 2000). In this context as well, the four sources of efficacy described by Bandura prove to be effective targets for interventions

to foster increased perceived self-efficacy. In particular, several studies have shown that how increases in self-efficacy higher levels of academic performance can be achieved through peer modeling, monitoring (by a teacher or by oneself), and providing evidence of growing abilities.

In a study conducted by Schunk, Hanson, and Cox (1987), children who struggled in math were exposed to peer models who demonstrated either rapid or gradual acquisition of a math skill. The students in the study seemed judge their own competence to be most similar to that of the peer models demonstrating gradual skill acquisition, and the students who observed these models experienced increased self-efficacy and performance. Schunk and Zimmerman (2007) reported on a similar study in which modeling was shown to be a successful means of raising elementary students' self-efficacy, reading comprehension, and writing skills. These studies provide examples of successful instruction to increase students' self-efficacy in two different academic areas. In both, vicarious experience, specifically live modeling, was used.

Another example of increasing self-efficacy in the academic context utilized monitoring during training. Schunk (1982) showed that children with low math skills who received both didactic instruction and practice opportunities, accompanied with either self-monitoring or monitoring by a teacher increased in perceived self-efficacy, skill, and persistence, while students who did not experience the monitoring did not experience the same growth in those areas. It is probable that self-efficacy increased as students who received the monitoring during training were made aware of their own progress.

Other research by Bandura and Schunk (1981) demonstrates a connection between setting proximal goals and increases in self-efficacy. Students with low ability and interest in math who were made to set proximal goals made significant increases in their abilities, interest, and self-efficacy in math. This finding suggests that providing encouraging learners to set proximal goals

helps them see evidence of their own growing abilities, thereby fostering self-efficacy and breeding greater academic success (Bandura & Schunk, 1981; Zimmerman, 2000).

This section has summarized several proposed modes of induction of efficacy expectations and has given brief overview of studies in self-efficacy and various methods for providing educational contexts and tools (i.e., mentoring, monitoring, and training in goal-setting) which helped increase students' self-efficacy in academic settings. It is important to note that, while self-efficacy is an important predictive factor to academic success, it also influences students' choice of major and perseverance in their chosen course of study, a lack of self-efficacy can be overcome through appropriate educational means (Zimmerman, 1995). The general concept of overcoming challenging academic situations will be discussed next.

Education and Academic Resilience

While awareness of stereotypes and low self-efficacy are certainly challenges that may be experienced specifically by girls in cybersecurity classes, there is also the broader issue of resilience in an academically challenging environment. Why do some student seem to thrive in academically challenging environments, while others shy away or become discouraged? Is there a way to increase this sort of resiliency and help children be more optimistic when acquiring knowledge or skills becomes difficult? This section will discuss some of the research that seeks to addresses these questions.

Diener and Dweck (1978) described two categories of responses that children demonstrate after experiencing failure: the "helpless" or maladaptive response, and the "mastery-oriented" response, focusing on how to overcome the failure. These two response patterns have been examined in numerous studies, which have indicated that the helpless response yields to an avoidance of challenge and a decline in performance when confronted with obstacles, whereas

the mastery-oriented response leads to seeking challenging tasks and exerting greater effort when faced with obstacles (Diener & Dweck, 1980; Dweck, 1975; Dweck & Leggett, 1988).

Blackwell, Trzesniewski, and Dweck (2007) studied a similar polarity in students' beliefs: in a longitudinal study, adolescents who held an "incremental theory" of intelligence (in other words, they believed that their intelligence was a malleable or changeable quality) were studied and contrasted with adolescents who held an "entity theory" of intelligence (in other words, these children thought of intelligence as a fixed entity). Researchers found that the incremental theory was positively associated with students' value of learning as a motivation, students' belief that effort leads to positive outcomes, and students' self-report that they would engage in positive, effort-based strategies in response to failure. After two years, the students who held the incremental theory performed better than students who held the entity theory in math, controlling for prior achievement.

In a second study, Blackwell et al. (2007) reported that an intervention designed to teach the incremental theory led to students to higher levels of classroom motivation (compared to a control group which did not receive the intervention), and also led to a reversal of the downward trajectory of students' math grades (again, compared to students in a control group with declining math grades, whose math grades continued to decline). This is a similar finding to other studies which have demonstrated that students' beliefs about their abilities and their response to failure can be changed with training: effective teaching can help students develop a more malleable perception of their abilities and a more adaptive response to failure (Dweck, 1975). Hence, while students clearly have differences in the ways that they respond to failure and their beliefs about their abilities, and these differences can significantly affect their academic

success, the maladaptive response and detrimental beliefs can be mitigated through training on the more productive belief patterns.

Dweck (2008), popularized the terms “fixed mindset” and “growth mindset,” which seem to encompass the ideas of the helpless response and the entity theory of intelligence verses the mastery-oriented response and the incremental theory of intelligence, to distinguish between the belief that one’s qualities, attributes, and aptitudes are fixed, and the belief that one’s capacity to learn and to develop skills and attributes can grow. Regardless of the terminology, the belief that one’s abilities can grow seems to be important for children to be successful in challenging learning environments and to persist in the face of obstacles. In the potentially challenging environment girls face in cybersecurity classes, this growth mindset seems essential for success. The good news is, this successful belief ideology is evidently teachable.

Current Interventions

I have outlined some of the external deterrents and internal barriers that cause women to be underrepresented in cybersecurity and have addressed the potential for education to mitigate some of the key challenges that girls may face in cybersecurity classes. Coming to an understanding of the deterrents and barriers that contribute to the underrepresentation of women in cybersecurity can hopefully lead instructors and advisors to implement successful interventions. Researchers have presented findings that suggest successful ways to increase women’s retention in STEM fields. Regular writing assignments on the utility value of subject matter has been shown to increase student interest and achievement in STEM fields at both secondary and post-secondary levels (Hulleman & Harackiewicz, 2009). Summer enrichment programs for students between their first and second years of college increase interest and motivation and help retain students in STEM programs (Linnenbrink-Garcia et al., 2018). By

taking such measures as including social impact and real-world application content in first-year computer science curriculum, providing research opportunities to women in the summer after their first year, and increasing the number of female faculty members, Harvey Mudd College and Carnegie Mellon University were both able to successfully increase the proportional number of women in their computer science programs in the 2000s (National Science Board, 2016).

Programs specifically designed to channel students toward cybersecurity careers have gained popularity in recent years. Specifically, cybersecurity competitions, both geared toward youth, such as the Air Force Association's CyberPatriot program, and hosted by computer science colleges for undergraduate students, provide the opportunity for students to work as a team and utilize cybersecurity skills in a competition setting. However, these competitions, while excellent opportunities for proficient students, require a high skill level in many different areas of cybersecurity, and are therefore ineffective, if not detrimental, for students with little to no experience to the field (Cheung, Cohen, Lo, Elia, & Carrillo-Marquez, 2012). In a report of initial results of a study on the National Cyber League, Tobey, Pusey, and Burley (2014) reveal that cybersecurity competitions may be better at engaging students already committed to the cybersecurity field than attracting students with little background experience and building interest.

These existing attempts to promote cybersecurity among students are failing at overcoming the barriers that are keeping women from the field. Far from overcoming the existing stereotypes, these competitions promote a hacker-style mentality. Furthermore, they do not foster self-efficacy in students without prior experience or with minimal experience.

In light of this lack of appropriate opportunities for novice students to develop interest in cybersecurity, a team from Brigham Young University has developed an intervention targeting

students without previous cybersecurity experience and designed to combat detrimental stereotypes and build self-efficacy. The intervention we have developed and will test in this study incorporates aspects of Alternate Reality Games (ARG's) and Virtual Internships, which will be discussed in the next section.

How Virtual Internships and ARG's May Contribute to Interventions

Shaffer (2006), used the term epistemic games to describe the "possible mechanism through which sufficiently rich experiences in computer-supported games based on real-world practices may help students deal more effectively with situations in the real-world and in school subjects" (p. 223). Chesler et al. (2015) used Shaffer's epistemic frame theory to introduce a new educational platform: the virtual internship. Chesler et al. (2015) show how virtual internships can be a valuable and enjoyable educational experience, allowing students to take on the role of a professional before they have sufficient skills and experience to do so in a real-life setting, and how these virtual internship experiences can lead to increases in career intent and self-efficacy. Arastoopour, Chesler, & Shaffer (2014) found that women, having participated in an epistemic game allowing them to become part of authentic engineering design teams, experienced an "increase in confidence in and commitment to engineering" (p. 211). Interestingly, these same findings did not extend to the men in the study, suggesting that women in particular may be motivated to persist in engineering by authentic simulations.

Similarly, a genre of simulation known as Alternative Reality Gaming (ARG), allows for participants (players) to take on a fictional role while interacting with other players through tools and messages that are embedded into their everyday lives (Bonsignore, Hansen, Kraus, & Ruppel, 2013; Jagoda, Gilliam, McDonald, & Russell, 2015; Niemeyer, Garcia, & Naima, 2009). The signature characteristic of ARG's is the "This is Not a Game" (TINAG) culture, which

allows players to suspend belief that they are playing a game and interact with the virtual environment as if it were real life. TINAG ethos is supported through these authentic, embedded means of interaction, but violated through interactions and interface forms that participants perceive to have been fabricated. Traditionally, ARG's are tied to a one-time event, often driven by an entertainment or marketing goal (Hansen, Bonsignore, Ruppel, Visconti, & Kraus, 2013).

This study explores the possibility that newer forms of computer games may hold the promise of informing new kinds of interventions which will allow students with little cybersecurity background to have meaningful and enriching experiences with cybersecurity activities that could lead to increased perceived self-efficacy in their ability to succeed in future cybersecurity activities, coursework, and even careers. The next section will discuss the simulation genre used in this study and how it incorporates aspects of virtual internships and ARGs for an educational purpose.

The Playable Case Study

At BYU, a new educational platform has been developed, incorporating aspects of epistemic games (Shaffer, 2006) and virtual internships (Chesler et al., 2015) to allow inexperienced students to take on a professional role with aspects of both a simulated online environment and in-class activities and lessons facilitated by a teacher to provide educational scaffolding. This interactive simulation, which allows students to take the role of a member of a professional team in an authentic scenario, is called the Playable Case Study, or PCS (Balzotti, Hansen, Ebeling, & Fine, 2017). The simulation poses a real-world problem associated with the professional discipline under study and unfolds in the form of a fictional story. Students interact with other team members, clients, disciplinary experts, or the public (all of whom are characters in the story) to solve the problem in an authentic manner. Students are also full participants in

the developing narrative and have opportunities to influence the direction the story takes, as well as the form in which they solve the problem under consideration.

The PCS is also similar to ARGs in that they strive to uphold TINAG culture by utilizing authentic means of interaction as much as possible. Students interact with the story's fictional characters via video-conferencing, email, texting, chatbots, file sharing, and other disciplinary modes of communication. Unlike traditional ARGs, however, the PCS has clear educational goals and associated classroom activities and may be run more than one single time.

Research on an earlier PCS reveals that students find this educational mode to be interesting and fun, and that students engage with the narrative and have emotional responses to the fictional characters (Balzotti & Hansen, 2019). This initial PCS was developed for the field of technical writing, and these attributes of this unique educational platform are certainly needed in an intervention that should enable students to take part in enriching activities that will counter some of the stereotypes about cybersecurity and build self-efficacy.

Conclusion

In this literature review, I have presented the current problem of underrepresentation of women in cybersecurity careers and outlined some factors which may contribute to the lack of both girls in cybersecurity-related fields of study and women who remain in cybersecurity careers. These factors include external barriers, including lack of support, encouragement, and peer mentoring, and alienation at recruiting events, unequal opportunities in the workplace, and feeling undervalued. There are also internal factors that play a part in deterring women from cybersecurity-related careers, including a mismatch between personal values and perceptions of the job, prevalent stereotypes, feelings of stereotype threat, and low self-efficacy.

I have also presented literature which supports the ideas that some of these internal factors, including the effects of stereotype threat and low self-efficacy, can be mitigated through education, and that the belief that capabilities are malleable and that new skills can be obtained can also be developed and promote greater academic resiliency.

Furthermore, I have described some of the current interventions for attracting more students to cybersecurity and how these current interventions are insufficient in attracting new, inexperienced students who may have low self-efficacy to the field. I have described the potential for virtual internships and ARGs to be used in interventions. Finally, I have described a new intervention developed at BYU and its potential to help mitigate some of the internal factors that deter girls from studying cybersecurity and to contribute to the efforts of raising interest and developing self-efficacy of girls in the field of cybersecurity.

CHAPTER 3

Method

In this chapter, I will present the intervention used in this study: the Cybermatics Playable Case Study, designed with the hope of increasing teenage girls' interest in cybersecurity and their confidence in their ability to succeed in a cybersecurity program. I will also describe the study participants, settings, and procedures used to collect observation and survey data which I use to address my research questions.

Cybermatics Playable Case Study

The Cybermatics PCS is structured around five simulated days in the professional life of a penetration tester, or an "ethical hacker," who is hired by companies to look for possible insecurities in their corporate networks. On the first day, students are hired into a cybersecurity firm known as Cybermatics and are assigned to a team beginning a penetration test for a home automation company called RipTech. The goal of the test is to try and breech RipTech's systems and identify vulnerabilities that can be patched. Throughout the simulation students complete a number of technical tasks including performing an SQL injection, cracking passwords, finding hidden files in a Linux system, and reporting the results of their work. By completing each simulated day within the PCS, students learn the terminology, the technical skills to complete assigned tasks, and the soft skills of working in a penetration test environment. All of these are situated in an authentic, albeit simplified, environment patterned after actual penetration testing teams. Tasks for each day are assigned by the team's lead character and completed through a simulated set of tools, including (a) video conferencing (pre-recorded video segments); (b) a documentation section for code documentation and training guides; (c) a chat messaging system

(actually a simple chatbot); (d) a Terminal shell for running Linux commands; and (e) a reporting section for co-authoring the final penetration testing report.

We have already collected data from running the Cybermatics PCS in various college Information Technology and Information Science classes at two universities. We were able to report on the data from 76 students, 65.8% male with an average age of 20, the majority of which were either studying or exploring Information Technology or Information Science majors. We found that the Cybermatics PCS helps college-level students gain a better understanding of the skills and traits needed to be successful in the field of cybersecurity, decide more firmly whether or not to pursue a career in cybersecurity, and develop greater confidence in their ability to succeed in a career in cybersecurity (Giboney et al., 2019).

As the PCS is designed to be an introduction to Cybersecurity, and as high schooler's interests are a strong predictor of later career choice, we are interested in expanding the Cybermatics PCS's target audience to include high school students. This study is first time that the Cybermatics PCS has been run in middle and high school classes. I specifically collected data from the girls in 9th-12th grade classes to answer the research questions.

Participants

Two classes used the PCS during the winter 2019 semester. One was a 9th grade technology class at a middle school in suburban Utah Valley. In this class, there were approximately 32 students, ages 14-15, of whom eight were female; the parents of seven of the girls in the class gave consent for their daughters to participate in the study. We also obtained assent from the students participating. The Institutional Review Board (IRB) approval letter, parental consent form, and child assent form used in this study are included in Appendixes A-C. These students had elected to be in a technology-oriented class, suggesting that they have some

interest in learning about technology. The other class was a high school computer science class, also in Utah Valley. In this class, there were 18 total students, of which three were girls. Two of these female students, ages 16 and 18, participated in the study from this class. Again, these students had elected to take a technology-oriented, or, in this case, specifically a computer science course. These classes had both male and female students. Both teachers implemented the Cybermatics PCS into their classroom curriculum so that all students in the class experienced the simulation. Data was collected from both male and female students, however, due to the specific research questions of this study, only data from the girls who participated in the study are presented in this thesis. They are referred to by pseudonyms when referenced individually.

Settings

My aim in this study was to test the PCS with high school-age students. This generally includes 9th-12th graders. However, in the particular school district where I ran this study, 9th graders attend junior high, and the high school includes 10th-12th grades. Therefore, I ran the study in a 9th grade class in a junior high school and a high school class of mixed grades.

Both the middle and high schools were on an A day/B day schedule, meaning that, instead of every class meeting every day, each class meets every other day, but for a longer period of time. In a two-week period, each class met five times, in which time we intended to coordinate each class period with the tasks of each of the five simulation days. This worked in the high school class. The 9th grade class ended up falling behind and needing an additional week to catch up on the simulation tasks.

Research Design

This research study utilized a mixed-methods approach. This allowed for the collection of quantitative data to address overall trends and determine if there were overall trends in how

the PCS influenced girls' interest and/or self-efficacy in cybersecurity. The qualitative data collection allowed for a more complete understanding of how the PCS was influencing girls on an individual level, accounting for the nuanced differences between experiences and greater emotions and insights that cannot be captured as richly, or is more difficult to capture, through the quantitative data.

Measures. Built into the PCS is a welcome survey. The survey is in-game, meaning that it is part of the simulation activities. Although all the students in the class participated in the in-game activities, including the survey, only survey data from the female students who have given assent to be included in our research study and whose parents have given formal consent for their children to be research subjects were analyzed.

The pre-survey questions are listed in Appendix D. They include five questions, presented on a 7-point Likert scale (1 = not at all true of me to 7 = very true of me), adapted from the Motivated Strategies for Learning Questionnaire (Pintrich & De Groot, 1990), and three questions on the same 7-point Likert scale relating to interest in cybersecurity. The pre-simulation survey also included an open-ended question relating to the students' perceptions of cybersecurity professionals.

These same questions were given to participants in an exit survey as they complete the Cybermatics simulation, along with questions about the students' experience with the simulation, whether they think the simulation helped increase their confidence in their ability to do well in a cybersecurity class in the future, and questions relating to how successfully the students felt they were able to complete the simulation and how enjoyable they found the simulation. The post-survey questions are included in Appendix E.

After the 9th grade students completed the simulation, I ran a focus group with the seven female participants, asking further questions about their experience with the PCS, and their thoughts on how their interest and confidence in their ability to do well in cybersecurity had been affected by their participation with the PCS. I explored these same issues in individual semi-structured interviews with the two girls in the high school class after their participation with the PCS. The general prompts of the focus group and interviews are included in Appendix F. The focus groups and interviews were recorded for later transcription. I

Procedure. I met with the teachers participating in the study prior to their using the PCS in their classes to familiarize them with the PCS layout and tasks. They presented the PCS to their students. I was present in almost every class period in which the simulation was run to take note of any challenges the students encountered and to assist where needed. Specifically, I took observation notes of the manner in which the teacher incorporated the PCS into the class; any scaffolding provided by the instructor; the general classroom atmosphere and student activity; comments and questions the students had relating to the PCS; and the students' overall reactions to the PCS, including parts of the PCS that they seemed to like, or that seemed to frustrate them.

The PCS has five simulation "days," with specific instructions from the fictional characters, further plot development, and tasks to accomplish on each "day." The tasks for Day 1 included the pre-simulation survey, and the tasks for Day 5 concluded with the post-simulation survey. Although the teachers had the option to assign PCS tasks as homework, both teachers gave the students the majority of class time during the unit to work in class on the simulation. Within a week of the conclusion of the simulation, girls from the junior high class were invited to participate in a focus group. The two high school girls were invited to participate in individual

interviews, which were conducted between one and three weeks after their class concluded the simulation. Both the focus group and the interviews followed a semi-structured format.

Data Analysis

Quantitative analysis. Following data collection, the students' pre- and post-survey data was compared to determine whether or not the students' perceived self-efficacy increased after interacting with the PCS. This was done by calculating the Pearson correlation between the responses of the five self-efficacy questions and assigning each student an overall self-efficacy (SE) score by averaging student responses on both the pre- and post-survey self-efficacy questions that had a high correlation with one another (each student was given two scores: pre-PCS and post-PCS). A paired-samples t-test was calculated on the pre- and post- simulation survey questions relating to interest and on the SE scores to determine whether or not there is a significant difference between the students' pre-and post-survey SE scores. Additionally, Pearson correlations were calculated on the post-simulation SE scores, interest questions, and questions regarding successful completion and enjoyment of simulation activities.

Qualitative analysis. The focus group and interview recordings were transcribed and analyzed using the constant comparative method described by Glaser (1965, p. 436-445). The transcriptions were coded to capture themes of the particular interviewee's experience, and/or themes reflecting commonalities amongst the girls who participated with the PCSs, particularly in relation to the students' overall experience with the PCS, interest in cybersecurity, self-efficacy, and perceptions of how interacting with the PCS may have affected those latter two constructs. The coded statements were studied for their coherence to each other and for the unique insights they provided. The open-ended responses in the surveys were also studied and compared to the themes found in the interview and focus group transcriptions.

CHAPTER 4

Findings

In this study, we hoped to find evidence of how the PCS affected the girls' interest in cybersecurity and self-efficacy in their ability to do well in a cybersecurity program. Between the two classrooms that ran the PCS during this study, nine girls participated in the study. Eight of the nine completed both the pre-simulation survey and the post-simulation survey. In our analysis of the quantitative survey data, we report only on data from the eight girls who completed both surveys. Seven girls, all from the same class, participated in a focus group after the simulation, in which a researcher asked questions about their overall experience with the PCS. Only two girls participated in the study from the other class that ran the simulation. Due to there being only two girls in this class, and to the fact that these two girls had quite different personalities, it seemed most appropriate to interview these students individually.

The quantitative findings revealed no significant difference in interest and self-efficacy scores between the students' pre- and post- simulation data. However, significant correlations were found to exist between students' post-simulation interest in cybersecurity, self-efficacy, and successful completion and enjoyment of simulation activities.

The qualitative data taken from the focus group and interviews provided further insights into how the experience with the PCS may have affected the girls who participated and how they perceived their experience with the PCS; the complexities of the constructs of interest and self-efficacy when measured in a group of adolescents lacking previous experience in cybersecurity, and how these constructs are being influenced heavily by various other factors outside the scope of this study; and the considerations that should be made when designing interventions for young audiences with little to no prior exposure to the intended subject matter.

Quantitative Findings

Of the five questions adapted from the Motivated Strategies for Learning Questionnaire (Pintrich & De Groot, 1990), four questions yielded student responses that were found to have a strong correlation ($r(6) > 0.75$, $p < .05$) to each other, based on the pre-simulation survey. The responses to "I expect that I could do very well in a cybersecurity class" had the weakest correlation to the other questions and were omitted from further analysis. The correlation statistics for the self-efficacy (SE) questions are shown in Table 1.

The student responses for the remaining four SE questions, including "I am sure I could do an excellent job on the problems and tasks assigned in a cybersecurity class," "I'm certain that I can understand the ideas taught in a cybersecurity course," "I think I would receive a good grade in a cybersecurity class," and "I know that I will be able to learn the material taught in a cybersecurity class," were averaged for each student, and each student was given an overall SE score based on that average. SE scores from the pre-simulation survey ranged from 3.5 to 6.0 (on a scale of 1-7). The SE scores from the post-simulation survey ranged from 1.3 to 7.0. Average SE scores, standard deviations, and paired-samples t-test results are shown on Table 2.

The same standard statistical analyses were run on the three questions relating to student interest. Those results are also shown on Table 2. While the results hint at a possible decline in interest and SE score, they are not significant. Therefore, with this quantitative data, we cannot reject the null hypothesis that the PCS does not affect student interest in cybersecurity or self-efficacy in their ability to do well in a cybersecurity class.

Table 1

Pearson Correlation for Pre-Test SE Questions.

	I expect that I could do very well in a cybersecurity class.	I'm certain that I can understand the ideas taught in a cybersecurity course.	I am sure I could do an excellent job on the problems and tasks assigned in a cybersecurity class.	I think I would receive a good grade in a cybersecurity class.
I'm certain that I can understand the ideas taught in a cybersecurity course.	0.52 p=0.187			
I am sure I could do an excellent job on the problems and tasks assigned in a cybersecurity class.	0.55 p=0.158	0.90 p=0.002*		
I think I would receive a good grade in a cybersecurity class.	0.68 p=0.064	0.93 p=0.001*	0.94 p=0.001*	
I know that I will be able to learn the material taught in a cybersecurity class.	0.75 p=0.032*	0.79 p=0.020*	0.78 p=0.022*	0.80 p=0.017*

*significant at $p < .05$

Table 2

Statistical Analyses of Eight Student Responses from Pre- and Post- Simulation Surveys.

	I am interested in cybersecurity.	I would like to learn more about cybersecurity.	I plan on taking a cybersecurity class in the future.	SE score
Average pre-simulation survey response:	5.0 (±1.3)	5.4 (±1.5)	3.6 (±1.8)	5.1 (±1.1)
Average post-simulation survey response:	4.6 (±2.0)	4.8 (±1.8)	3.8 (±1.7)	4.4 (±1.7)
Net change (avg. post - avg. pre)	-0.38	-0.63	+0.13	-0.65
Paired-samples t-test	-0.513 p=0.623	-1.11 p=0.305	0.357 p=0.732	-1.38 p=0.209

*significant at $p < .05$

Correlations between the interest questions, the SE score, and a question relating to the students' successful completion of the simulation were also calculated. A high correlation was found between responses to all the questions tested, except for "I plan on taking a cybersecurity class in the future." In other words, the data indicate that self-efficacy score, interest in cybersecurity, interest in learning more about cybersecurity, enjoyment of the simulation, and successful completion of simulation tasks are all correlated. The results of these analyses are shown on Table 3. These results indicate that students who enjoy the simulation and who feel they have been successful in completing the simulation tasks also express interest in cybersecurity, a desire to learn more about cybersecurity, and a high SE score.

Table 3

Post-Simulation Response Correlations.

	I am interested in cybersecurity.	I would like to learn more about cybersecurity.	I plan on taking a cybersecurity class in the future.	SE score	I was able to complete the tasks assigned to me at Cybermatics effectively.
I would like to learn more about cybersecurity.	0.95 p=0.000*				
I plan on taking a cybersecurity class in the future.	0.74 p=0.036*	0.81 p=0.016*			
SE score	0.90 p=0.002*	0.94 p=0.001*	0.84 p=0.009*		
I was able to complete the tasks assigned to me at Cybermatics effectively.	0.76 p=0.027*	0.75 p=0.032*	0.40 p=0.327	0.76 p=0.028*	
I enjoyed my time at Cybermatics.	0.85 p=0.008*	0.81 p=0.016*	0.66 p=0.075	0.89 p=0.003*	0.83 p=0.012*

*significant at $p < .05$

Qualitative Findings

The focus group and interviews provided further information on how the girls perceived their experience with the PCS and how they felt it affected them.

Reactions to the Playable Case Study experience. Overall, the girls thought the simulation was "fun," but many also expressed frustration and feeling like they didn't know what they were doing, or if they were doing the right thing during the simulation. When asked what was fun about it, their responses included "password cracking," "Linux," and "it made me feel like a secret agent." However, girls also made comments that revealed feelings of confusion and helplessness, such as "I have no clue how to use that!" and "I don't even know what I'm doing!" This mixed experience was well-captured by one girl's comment, right at the beginning of the focus group: "I think it was pretty enjoyable. I gotta admit, it'd get frustrating at times, when I was like, 'What am I doing wrong?!' But I think overall, the whole experience was fun." This seemed to be the general sentiment expressed by many of the girls: that the simulation was enjoyable, but also, at times, frustrating.

It seemed that the complexity and ambiguity of the simulation tasks went beyond students' anticipations. As an example, one of the simulation tasks requires students to use a hash cracking command in a simulated Linux terminal to crack a list of password hashes one at a time. Many students did not realize at first that they needed to try to crack all of the passwords before moving onto the next task. Of this simulation activity, one student commented, "It took forever! And I didn't understand ... I thought I had to figure out really quick how to get the passwords, but then it wasn't working for me." This student's response indicates that she was expecting to be able to find a quick solution to a task that ended up taking a considerable amount of time. In the post-simulation survey, several students offered suggestions of how the PCS

experience might be improved for future students. "Have more clear directions and instructions," one student said. Another student responded, "Being more specific in what they wanted to be done." These two students' comments reflect a desire for more straightforward instructions on simulation tasks, many of which were intentionally created to be somewhat ambiguous and rigorous to create a more realistic experience. It seemed that students were expecting quick, straightforward solutions to the simulation tasks, and that the activities were actually more time-consuming and complex than they expected.

The girls who were interviewed and who were in the focus group revealed several things about what they felt was most effective in helping them learn and have a successful experience with the PCS. They generally wanted a chance to work out the tasks of the simulation on their own but wanted to be able to ask for help (generally from an instructor) when they needed it. They wanted help in the form of hints that would still allow them to figure things out on their own. One girl explained her process of working through some of the more challenging tasks of the simulation: "I'd work on things by myself, trying to figure it out on my own … if I was stuck, I would ask for help. … I would usually like it if [the help I received] was like a hint, and not just like directly what the answer was. … After I got the hint, I would … see if I could use that to figure everything else out by myself."

Being able to actively figure things out in the simulation led to the opportunity to experience the achievement of finding the correct answer or solving the problem assigned in the simulation. This achievement seemed to be something that the girls found rewarding, and they were disappointed when that rewarding experience was taken away. In one case, the teacher gave an answer to the entire class that some students were close to discovering on their own. Of this experience, one student commented, "I like to get the answer by myself. I like to do the

work for it. And if I've already been doing the work for it, and you just give me the answer, that just kinda throws all my work out the door." Another student did not get all the way through the simulation, due to classroom time restrictions, and so she never was able to complete the final tasks. "We were sad when it ended," she said.

Girls in the focus group also talked about how they felt they learned better by doing than by reading information that did not have an immediate application to a simulation task. The PCS had a documents section that gave more information relating to the tasks that the girls were asked to do. The girls in the focus group talked about how they felt like they learned better by applying the information from that section than by just reading it. With regards to the section of the documentation that went over Linux commands that were needed in the simulation, one girl said, "I didn't really understand what anything meant, but … it just made sense when I was doing it." another girl said, "I feel like you learn better as you use [the information]."

In summary, the students' reactions to the simulation reveal that they felt the simulation was both fun and frustrating and suggest that the simulation was also more rigorous and ambiguous than the students were expecting. The students' comments also indicate that they wanted both autonomy and the availability of hints when needed, but ultimately, they wanted to feel the satisfaction of having found the solutions to the simulation tasks. Lastly, comments from the focus group indicate that the students felt that they learned better by doing the simulation-based tasks than by just reading material in isolation.

Effects on interest and self-efficacy. The qualitative data of this study revealed that most of the students came into the simulation with no prior exposure to cybersecurity, that "interest" in cybersecurity was a construct that held a slightly different meaning to different students, and also suggest that the simulation may lead to greater self-efficacy, but that this

construct is also experienced in a complex and subjective way by the demographic studied. The following sections discuss these findings in greater detail.

Lack of prior experience. Of the seven girls in the focus group, only one said she knew anything about cybersecurity before the simulation. She said she had friends "going to school for that." The rest of the girls in the focus group, however, indicated that they knew essentially nothing about cybersecurity before interacting with the Cybermatics PCS. One girl in the focus group commented, "I had no clue about any of this stuff until now."

Because of this lack of previous knowledge or exposure, being interested in cybersecurity or feeling capable of learning about or doing cybersecurity work was not something most girls had thought about at all before the simulation. This is revealed in the way one of the girls talked about their perceptions of whether or not they'd be interested in or good at cybersecurity before the simulation: "I never even thought about it. The thought of liking cybersecurity, that hadn't even crossed my mind before doing this." Like this student, most of the girls in the study came to the PCS experience with essentially null interest and self-efficacy in cybersecurity.

Interest. Qualitative data indicate that the PCS did lead to increased interest in cybersecurity. The girls in the focus group unanimously indicated that they were more interested in cybersecurity after completing the simulation (two did not give verbal responses). As indicated by one girl's comment, the greater interest in cybersecurity seemed to be somewhat of a pleasant surprise to many of the participants: "Before [the simulation] I'd be like, cybersecurity? I'm good [meaning, "I'm fine with not being involved in it at all."]. But now I'm like, I actually kinda enjoyed that." Four of the seven girls from the focus group reported in the post-simulation survey that they are interested in cybersecurity. One did not complete the post-survey. One said she was not interested because "it's too much for me."

This comment, “It’s too much for me,” reflects that this girl’s construct of interest seemed to be related to what she felt she was capable of doing, or her perceived self-efficacy. We found that as we used the term “interest,” the girls in the study actually seemed to be associating “interest” with slightly different constructs, as evidenced by the contrast between comments such as “I don’t really enjoy being on computers … This is not something I’d put my time and effort into at all, unlike with other stuff that I do,” from one student who was interviewed, Sari, and the comment “I’m not sure if I could do it,” from Morgan, another student interviewed, who actually did say that she enjoys spending free time on computer-based activities.

Self-efficacy. Most of the girls in the study expressed that the simulation increased their confidence that they could do well if they were to take a cybersecurity class in the future. No one said in either the focus group or in an interview that they thought the simulation made them *less* confident that they could do well, but one girl interviewed said that her interest and confidence in her ability to do well in cybersecurity were about the same after the simulation as before. This girl had the greatest change (decrease) in SE scores and the lowest SE score in the post-simulation survey. Two of the girls (one interviewed and one in the focus group) expressly acknowledged that the simulation did not teach them everything that they would need to know to be successful in future cybersecurity work, but they did feel that the simulation helped them feel more confident in their ability to learn more.

The comments from these students indicate not only that they knew little about cybersecurity before the simulation, but also that after the simulation, they felt like they know more about cybersecurity than they did before. One of the students interviewed commented that the simulation helped her see “how it’s done,” and brought up the teamwork aspect of the

simulation. The simulation seems to have affected the students by helping them gain some exposure to cybersecurity and what it would be like to actually do cybersecurity work at a very basic level.

Summary of Findings

While the quantitative findings of this study show no significant change overall in students' interest and self-efficacy in cybersecurity, the qualitative findings show that girls who participated in the simulation experienced a polarity of feelings toward the simulation; many found it to be both fun and frustrating; they wanted help to be accessible when they needed it, but also wanted a chance to problem-solve and experience success. The girls found the simulation to be more challenging than they anticipated, but liked to be able to learn by doing. The qualitative data also suggest that girls felt more interested in cybersecurity and greater perceived self-efficacy after participation with the simulation, and the quantitative data indicate that high interest, high self-efficacy, and a desire to learn more are all positively correlated with successful completion of Cybermatics tasks.

CHAPTER 5

Discussion

This study examined the effect of the Cybermatics PCS on high school girls' interest in and self-efficacy, specifically, what correlations may exist between using the PCS and high school girls' interest in cybersecurity and in their self-efficacy in their ability to do well in a cybersecurity class. While previous studies have been done on students' interactions with the Cybermatics PCS, this is the first time the PCS has been tested below the college level. Our findings reveal various complexities of creating and determining the impact of an intervention targeted to this younger, less-experienced demographic.

The quantitative results were insufficient to determine whether the PCS changed girl's interest in cybersecurity and self-efficacy from pre- to post-simulation (perhaps in part due to small sample size), but they did reveal meaningful correlations between interest, self-efficacy, successful completion of the simulation tasks, and overall enjoyment of the simulation. In other words, girls who had a positive experience with the simulation and believed that they were able to complete all the simulation tasks successfully also had a higher interest in cybersecurity and higher self-efficacy in their ability to do well in a cybersecurity class. Although our statistical measures cannot allow us to draw a causal conclusion, this finding highlights the importance of designing educational interventions that are enjoyable and that provide students, particularly female students, with experiences that they will perceive as enjoyable and that they will be able to complete successfully. If the aim is to increase interest and self-efficacy, these correlations reveal the necessity of making sure students are able to experience successful task completion in an activity that they find enjoyable.

Qualitative data provide additional insight into the girls' experience and their perceptions, culminating in several important findings: (a) many girls have little, if any, prior knowledge of cybersecurity; (b) there is great heterogeneity in the girls' concepts of interest; (c) the girls' self-efficacy is complex, and possibly interwoven with various other constructs and personal traits; and (d) the girls experienced some degree of enjoyment and satisfaction, but also frustration from various aspects of the simulation. These findings provide greater understanding of complexities of the experience the girls are having with the PCS and can inform future development and implementation of future PCSs and other similar interventions.

Lack of Prior Knowledge

In previous PCS research, students were given a pre- and post- simulation survey, which included questions about their level of interest and confidence in cybersecurity. Prior to this study, the students participating in the simulation studies were all college students nearing the end of the semester in a beginning Information Technology or Information Science class. Although many of these students had not had previous experience in cybersecurity, we can reasonably assume that their exposure to and general knowledge about the field was greater than the high school-age girls in this study, due to our findings that many students in our study knew essentially nothing about cybersecurity before the simulation. With this in mind, the conventional approach of asking pre-simulation questions to determine levels of interest and self-efficacy poses challenges for this less-experienced demographic. If a student has a baseline of zero in terms of what she knows about a subject, how does she say what her level of interest is? To try and decide whether she has low or high interest seems irrelevant in such a case. One might want to conclude that this student has a neutral interest, but that is not quite accurate, as neutral interest is not equivalent to null interest. Null interest would probably be the most

appropriate way to describe the level of interest someone has if they have not even thought about the subject matter in question.

Sari, one of the girls interviewed, said, "[Because of my class], I already knew what [cybersecurity] was for, but I didn't know … how it's done. … I didn't understand … like … hash cracking—never heard of that before this." For Sari, a question in the pre-simulation survey such as "I feel confident that I could crack password hashes," would seem strange and irrelevant. Sari's comment further demonstrates the complex implications of interpreting interest and self-efficacy of students who have such little prior knowledge of the subject matter, and how qualitative research measures provide insights that quantitative measures may be unable to capture. It may, in fact, be possible that the lack of significant change between pre- and post-simulation interest and SE scores in the quantitative data may be evidence of inaccurate self-reports of self-efficacy in the pre-simulation survey, due, in part, to lack of prior knowledge.

Furthermore, research has shown that people with low skill levels often overestimate their own competence on surveys (Kruger and Dunning, 1999). This phenomenon may cause difficulties in the comparison between pre- and post- survey results. Some students' survey responses on questions relating to their perceptions of self-efficacy decreased (the students expressed less confidence in their own competence and ability) after interacting with the simulation. While one explanation of this phenomenon could be that discouraging experiences with the PCS diminished the students' self-efficacy, another explanation could be simply that the lack of prior knowledge caused the girls to give an unusually high responses on the pre-survey questions.

Interest in Cybersecurity

Although most of the girls in the study indicated in the focus group and interviews that the PCS increased their interest in cybersecurity, it was evident that "interest" was not a consistent construct among all of the students. This was especially evident in comparing the comments from Sari and Morgan, the two students who were interviewed.

Sari's version of interest seemed to relate to her preference for what she cares to focus on, what she wants to learn about, practice, develop skills in, and potentially do professionally. At one point in the interview, she said, "I don't really enjoy being on computers." She indicated that other things come more easily and are more interesting to her than computers, so those other things are what she spends her time on. In other words, interest is more of a choice for Sari, as revealed in her statement, "This is not something I'd put my time and effort into at all, unlike with other stuff that I do."

It is interesting to note that Sari actually expressed in her interview that she would someday like to be an elementary school teacher. Traditionally, a teacher's role would be perceived as fulfilling communal goals, and so Sari's preference may seem in support of ideas by Diekman et al. (2010) that women gravitate toward more community-oriented careers. However, the assumption that Sari would favor being a teacher over being a security analyst because of a preference for communal goals cannot be supported by the data collected in this study. The conclusion that can be supported by the data is simply that Sari has other career plans, which could just as easily be due to previous exposure and positive associations with teachers (versus a lack of exposure to security analysts) as it could be due to a preference for communally-oriented careers.

In contrast, Morgan indicated that she *does* like computer-based activities, however, she said she is *not* interested in cybersecurity as a profession. When asked why, Morgan said, "I'm not sure if I could do it." For Morgan, interest seemed less a matter of personal choice, and more a reflection of what she sees a feasible option for her, given her skills and abilities. Not being sure she would succeed, Morgan is more cautious to say she is interested.

Just as Sari and Morgan seemed to have slightly different versions of the construct of interest, it is possible that, if we were to have similar discussions with more students, even more constructs would emerge from what we've called "interest." This possibility emphasizes the finding that that this idea of "interest," is much more complex and multi-faceted than can easily be captured by quantitative measures, as the very construct holds slightly different meaning to the different students who interact with the PCS.

Furthermore, while students might find the simulation or the subject matter interesting, they may not necessarily be personally interested in cybersecurity, which is an outcome influenced by factors well beyond the simulation experience. In their interviews, Sari and Morgan both shared ideas of what they would like to do professionally someday. If a student is already wanting to be an elementary school teacher someday, as Sari did, she probably will not be interested in cybersecurity. This lack of interest, so to speak, is a reflection of her personal preferences, thoughts, feelings, and experiences more than a reflection of how much liked the content of a five-day simulation. One girl in the focus group did, in fact, use the word "interesting" to describe what she thought of Cybermatics, but we cannot necessarily construe from that that she is interested in becoming a cybersecurity professional.

Self-Efficacy

Like interest, when asked about their thoughts on their ability to do well in a cybersecurity class after the simulation, the girls in the focus group indicated that they felt more confident that they could do well than they would have felt before the simulation. One of the focus group participants commented, "Before I thought that, there was no way, I mean, I always thought … hacking would be way too hard for me to ever do, and I was like, nope! But now that I realize that it's actually easier than I thought it was, it would be easier to adjust to it." This girl's perception that cybersecurity was actually easier than she thought it was initially was not shared by all the participants. Again, Sari and Morgan's interviews reveal significant differences in the girls' self-efficacy in cybersecurity after the simulation.

Morgan talked in her interview about how she liked gaming and wanted to learn stuff about coding for game development. She took a computer science class because she thought it sounded fun. In her interview after the simulation, however, she expressed that she definitely did NOT want to do cybersecurity professionally and didn't think she wanted to take a college class in cybersecurity either. When asked why, she said, "I'm not sure if I could do it." She was asked if cybersecurity would be interesting to her if she felt more confident. "If I felt more confident with it, yeah."

Morgan seemed to lack confidence in coding in general, even though her initial interest in learning coding had drawn her to taking the computer science class. "I don't feel like I'm good at it," Morgan said, "but, it is what it is. I don't think I'm that good, from what I've seen I mess up a lot of times, and I don't get code right, but eventually I get it right." later: "[other kids who are good at coding] they can do it really fast, but I'm just slow…I go at my own speed. [other kids in her class] they're just going fast cause that's just their own pace." Morgan's comment

carries a sentiment of resignation to a fixed reality that her skills and abilities relating to coding are less advanced than the abilities of other students in her class.

When asked what skills, responsibilities would be important for a cybersecurity professional, Morgan described specific skills of someone who seems very different from how she perceives herself: “Probably knowing exactly what they’re doing. And can show anyone what degree on what to do, like codewise, or how to hack, or basically any degree on that.” When asked if she thought she had these skills, Morgan said, “I’m not quite sure. I might. But I’m not sure.” Morgan seemed doubtful that she had the skillset that matched her perception of a successful cybersecurity analyst and seemed to have little confidence in her ability to grow her skillset. The cybersecurity professional persona seems out of reach of Morgan.

In contrast, when Sari asked about what skills, responsibilities would be important for a cybersecurity professional, she talked about attributes and characteristics of someone who could probably develop more of the specific skills: “They’d need to be trustworthy people that have really, really good ethics so that you know you can depend and rely on them. They should have a sharp and keen mind and be able to notice what is off that they need to report in. They should be able to work under [stress].” Sari had talked about the importance of ethics in her interview when she said, “Ethics in cybersecurity is basically like … how ethics should be everywhere. I’ve just kind of always known that from growing up that that’s what you need to be doing, and it’s not good if you’re not doing what you’re supposed to do.” It seems reasonable to construe, from Sari’s strong emphasis on good ethics, that she probably sees herself as possessing this particular attribute that she sees as being important to a cybersecurity professional. In other words, the attributes and characteristics that Sari sees as necessary for a success in cybersecurity seem, at least to some extent, to align with her own self-perception.

From her comments, it seems that the cybersecurity professional persona is not unattainable to Sari.

Furthermore, Sari seems to have a strong belief that skills can be obtained by practice. She said in her interview, “Because of [the PCS], I was able to go, okay, I can actually do this if I work at it.” She also talked about it in comparison to music and sports: “It’s kind of like sports or languages. … You are going to be better at it if you’ve been spending more time putting your time and effort into it.”

This sense of learn-ability, or belief that skills can be gained through practice and work, seems akin to the growth mindset described by Dweck (2008), and is something that another student in the focus group demonstrated: “It’s not so much like I already know everything, so I could do well in a class, it’s more like my confidence has like grown I guess because of doing this.”

From these statements and the contrast between Sari and Morgan’s perceptions, we gain greater insights into the complexity of the construct of self-efficacy. The students who participated in the same simulation came away with different perceptions of how difficult cybersecurity is and what skills are most important for a cybersecurity professional to be successful. They also demonstrated different levels of belief that they could learn new skills with time and effort. Therefore, self-efficacy seems to reflect on combination of affordances of the simulation and girl’s mindset, attitudes, and other personal characteristics.

Some of these differences demonstrated by Sari and Morgan seem to reflect the difference between the helpless and mastery-oriented response described by Diener and Dweck (1987), the mastery-oriented response being exhibited by Sari’s seeming belief that she could aquire the skills needed to succeed as a security analyst, and the helpless response being reflected

in Morgan's doubt that she could really "do it." Doubting her ability, or potential ability, to succeed will be a deterrent for someone like Morgan from pursuing further cybersecurity education. However, as Bandura (1977), Zimmerman (1995), and others have demonstrated, self-efficacy beliefs can be increased through various means. In efforts to encourage female students to learn more about cybersecurity, it may be beneficial to incorporate some means of promoting the belief that one's abilities can be developed outlined by Bandura (1977) or the growth mindset, described by Dweck (2008) in order to help students like Morgan develop greater self-efficacy and specifically feel more confident in her ability to successfully pursue further education in cybersecurity.

Our findings also suggest a possible interplay between interest and self-efficacy. Neither Morgan or Sari seemed to indicate a particularly high level of confidence in their ability to do well in a cybersecurity class in the future, or in a cybersecurity career. Interestingly, for Morgan, her apparent low self-efficacy seemed to stifle her interest in pursuing a career in cybersecurity. For Sari, who is not interested in cybersecurity, the question of how confident she would be in her ability to do well in a cybersecurity class seems irrelevant.

This speculation of an interplay between interest and self-efficacy drawn from the qualitative data aligns with the quantitative data, as interest in learning more about cybersecurity and in cybersecurity generally correlated in the post-simulation survey with SE score and with successful completion simulation tasks. This finding is fitting in the context of the greater body of self-efficacy research, which asserts that successful experiences lead to greater perceptions of self-efficacy, and interest is affected by perceived competence (Schunk, 1991).

Tension Between Fun and Frustrating

Our findings indicate that the simulation tasks were more rigorous, time-consuming, and ambiguous than many of the girls were anticipating, and that this unexpected complexity brought mixed reactions. In fact, two girls used the analogy of learning a new language in describing the learning process relating to their experience with the PCS, one to express her confusion, and another to express how the simulation made cybersecurity seem more interesting to her. Both are alluding to a greater challenge. A girl in the focus group said, "It almost has a completely different language. … You don't just type in English and it gives you an English response. It's like you're learning a language … and that kind of makes it more interesting to me. It makes it seem also a little more in-depth to me I guess." But while this girl felt that the novelty and complexity made the simulation more interesting to her, another girl spoke of the unfamiliarity in a more negative tone: "That stuff [using code, SQL, and password cracking] doesn't make sense to me, cause I'm having to do stuff that is not in the languages that I know."

While these students both found the tasks of the simulation to be new and complex, and both likened the experience to learning a new language, this aspect of the simulation experience was perceived very differently by the two students. Therefore, in trying to determine how the simulation as a whole, or even just specific aspects of the simulation, affect students, it is apparent that there will be very mixed reactions among students.

The girls in the focus group commented on the process of working through the tasks in the simulation: "It's not like just type in a few things and get all the answers, it's more of a play-by-play, like you've gotta do one thing, and then you've gotta move to the next." Her comment suggests that perhaps she and/or other students were expecting the tasks to be simpler and more straightforward, but also that she came to understand and anticipate the more complex process of

problem solving that the simulation required. Another girl talked about having to adjust to this process: "I feel like it's … an adjusting experience, like at first, you're probably not going to get anything at first, but I feel like, after a while, you start to sort of get it."

These comments seem to indicate a sort of progression or evolution of working through the simulation. At the basic level, there is a progression of the student working through the tasks, but also there seems to be a change in the student's experience as she gains a better understanding of the process needed to complete the simulation tasks. It seemed that this experience was frustrating at first; "not getting anything," according to the student's comment, would most likely be a discouraging experience.

However, as the students worked through the frustration and experienced success, the simulation experience seemed to become more rewarding. One student highlighted this aspect of the experience in her post-simulation survey response to the question "What did you like most about your time at Cybermatics?" Her response was, "trying things over and over again then being excited that finally something worked." This simple statement seems to capture both the potentially tedious and frustrating experience of trial and error, and then the satisfaction of finally achieving success, a tension which previous research has consistently shown to be prevalent in the PCS experience (McDonald, 2019). Similarly, when asked what they liked about the simulation, many girls in the focus group commented on the Linux terminal because it was "fun to experiment with" and because of its affordance of "trial and error." "It made me, well, trying things out, and then something finally worked, it made me a lot more happy, like, okay, I can actually do this, like, I'm going somewhere," one girl commented.

This experience of a potentially frustrating and discouraging process of trial and error culminating in a satisfying resolve demonstrates how a student could go through the simulation

and experience both frustration and enjoyment. It also shows how, depending on whether the student was able to actually reach the point of resolve when "something finally worked," the student's overall feelings about her experience may be very different.

This understanding of the complexity of the students' experience is important because we see how feelings of both fun and frustrating existing simultaneously and, when asked to make an overall judgement on her experience with the simulation on a Likert scale-style survey question, a high school student's mixed feelings may cancel each other out, losing the nuances and diversity of what she really experienced. Furthermore, as the high school students needed more classroom scaffolding to complete the simulation tasks than the college students who have tested the simulation in previous studies, their responses may be significantly affected by whether they were able to actually finish certain tasks and whether they received the scaffolding they needed to complete the tasks successfully. These possibilities could also provide insight into the lack of any significant change in students' interest in cybersecurity between pre- and post- simulation survey data.

Discussion Summary

In summary, we found that many of the high school girls came to the simulation with little background exposure to cybersecurity, and that designing and assessing an intervention for students so inexperienced poses unique challenges. The pre-simulation interest and self-efficacy for these students is essentially null. During the simulation, girls experienced both positive and negative emotions as they rotated through periods of struggle and moments of achievement. After the simulation, the constructs of interest and self-efficacy are affected by factors beyond the influence of the PCS, and the girls' experience with the PCS was so varied, that simply

reporting on changes in interest and self-efficacy is insufficient in describing the experience these high school students had with the PCS.

Based on correlations between enjoyment of simulation activities, successful completion of simulation activities, interest, and SE scores, we may speculate that the PCS has potential of increasing interest and self-efficacy in cybersecurity, but only for students who enjoy the simulation and who believe they have been successful in the simulation. However, the greatest benefit of the simulation could be simply in giving exposure, and, in the words of one of the participants, showing "how it's done," or what it would be like to actually be doing cybersecurity work, possibly breaking down some inaccurate stereotypes and conveying a more accurate view of the field.

Limitations

This study is limited in its scope due to the small sample size included in the study. The quantitative survey data would have greater potential for generalizable results had we been able to collect data from more students. However, the fact that only eight female students' data was available to us between the two classes in the study is indicative of the problem of low numbers of women pursuing fields relating to cybersecurity which this thesis attempts to address.

Another potential limitation of this study is the homogeny of the group of research participants. All students had elected to be in a technology-oriented course. It would be valuable to collect data from high school girls who may not have elected to enroll in a course connected in any way with computer science and cybersecurity for a more complete picture of how the PCS may influence a greater sample of the population of teen girls.

Additionally, there is the potential concern about the validity of both qualitative and quantitative data due to the research subjects not being completely truthful and thorough in their

survey responses and comments in the focus group and interview. It is quite possible that teenage students might not have a high level of focus and real intent as they take a survey. It is also possible that the girls in the focus group and the ones being interviewed might have attempted to give answers that they thought the interviewer was wanting to hear. However, since similar themes were discovered in the interviews and focus groups, and the responses of the students in the interviews/focus group seemed to align with the survey data, this possibility of faulty data does not seem to be of great concern in this study.

Finally, it is probably fitting to question whether this simulation, covering only a two- to three-week unit in the classroom, could actually permanently increase teenage girls' interest or self-efficacy in cybersecurity. While future research is needed to determine if such an intervention can produce lasting changes in these areas, the fact that the students who have taken part in the simulation are at least more familiar with cybersecurity concepts will certainly be an advantage to them at a future point if and when they are given another opportunity to learn more about cybersecurity.

Implications for Future Research

While data from both male and female students were collected in this study, only the data from the female students were used to answer the research questions of this study. Future research is needed to determine whether the findings reported in this study are consistent with the data from the male students.

One important theme of the findings had to do with scaffolding: students wanted help to be available when needed, but also wanted to be able to experience achievement for themselves. This dichotomy creates a scaffolding challenge. Future research can examine appropriate levels of scaffolding and how to provide scaffolding appropriate for students at different levels of

ability, working at different paces. Future research may also examine strategies that may be used to provide appropriate scaffolding without taking away the learner's autonomy. This extends not only to the diverse needs of a single classroom, in which students possess varying levels of ability and motivation, and if left to their own, will surely work through the simulation at different rates, but also to the diverse classes in which Cybermatics may be used. We have now tested various versions of Cybermatics in middle school, high school, and college classes. If the Cybermatics PCS will be used for a broad audience, then it will most certainly need varying levels of scaffolding available.

Finally, the classroom setting poses many challenges. In just the two classes participating in this study, vast differences were observed in how the teacher implemented Cybermatics. Further research could be done to determine best practices in teacher implementation.

Implications for Practitioners

The results of this simulation bring to light some of the complexities of trying to determine changes in interest and self-efficacy for students who have no baseline understanding of the subject matter. Although designing for these novice students does involve complex implications, such simulations have the opportunity to give exposure, break down stereotypes, and help students develop an accurate concept of the field and subject matter while providing an enjoyable experience. Practitioners might focus their efforts on giving students exposure to the field, thereby helping students gain an accurate perception of cybersecurity; and on facilitating a positive experience with the subject matter, ensuring appropriate scaffolding to help the students have both the help and the challenge they need to feel both satisfied in their accomplishments and reassured in their ability to succeed.

It may also be beneficial to consider how to promote self-efficacy and the development the growth mindset or mastery-oriented response patterns described by Bandura (1977), Dweck (2008), and Diener and Dweck (1978). Incorporating such elements in the design of future interventions may help girls develop greater self-efficacy in their ability to do well, or their ability to acquire the skills needed to do well, in cybersecurity tasks, classes, or even careers. Ultimately, this may help increase girls' likelihood of pursuing further education in cybersecurity.

CHAPTER 6

Conclusions

This thesis has reported on a study designed to examine the experience of teenage girls who participated in the Cybermatics Playable Case Study, an intervention designed to help increase students' interest in cybersecurity and their self-efficacy in their ability to do well in a cybersecurity class, program of study, or career. This study also examined how, if at all, the experience with the Cybermatics PCS affected the girls' interest in cybersecurity and their ability to be successful in a cybersecurity class.

Quantitative findings indicate correlations between successful PCS completion, enjoyment of the PCS, interest in cybersecurity, wanting to learn more about cybersecurity, and self-efficacy. Quantitative data reveal several key findings, namely, (a) many teenage girls know little about cybersecurity, and therefore make a very meaningful judgement on their initial interest and perceived self-efficacy; (b) the construct of interest is heterogenous; being "interested" or "not interested" in cybersecurity is a conclusion reached by various influences and holds different meanings for different girls; (c) self-efficacy in ability to do well in a cybersecurity course is also a complex subject, perhaps influenced by personal traits and other beliefs and constructs; and (d) the girls generally had mixed reactions to the PCS and experienced both enjoyment and frustration and wanted both help and autonomy at various points in the simulation.

These findings are informative to future researchers and practitioners. First, it is important to note the lack of prior knowledge and experience that participants had coming into the simulation. Researchers should be mindful of this in any baseline data they attempt to collect, and practitioners should be aware that their greatest success in designing an intervention

may be simply in giving realistic exposure to the field of cybersecurity. Furthermore, it would be wise to try to scaffold interventions to minimize frustration and make the successful completion of the simulation maximally achievable, providing opportunities for help or hints at appropriate times, but not when unwanted. The appropriate level of scaffolding will be different for different classes and even different students, and further research is needed to determine how best to provide this type of personalized scaffolding, either within the simulation or in the classroom instruction.

References

Arastoopour, G., Chesler, N. C., & Shaffer, D. W. (2014). Epistemic persistence: A simulation-based approach to increasing participation of women in engineering. *Journal of Women and Minorities in Science and Engineering*, *20*(3), 211-234.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, *12*(1), 24-31.

Balzotti, J. & Hansen, D. (2019). Playable case studies: A New Educational Genre for Technical Writing Instruction. *Technical Communication Quarterly, 8*(2), 1-15. doi: 10.1080/10572252.2019.1613562

Balzotti, J., Hansen, D., Ebeling, D., & Fine, L. (2017). Microcore: A playable case study for improving adolescents' argumentative writing in a workplace context. In *Proceedings of the 50th Hawaii International Conference on System Sciences*. Retrieved from https://pdfs.semanticscholar.org/1cf2/0e3555daa98d89b3b7754f79e945ad125361.pdf

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191-215.

Bandura, A., Barbaranelli, C., Caprara, G. V., & Pastorelli, C. (2001). Self-efficacy beliefs as shapers of children's aspirations and career trajectories. *Child Development*, *72*(1), 187-206.

Bandura, A., & Schunk, D. H. (1981). Cultivating competence, self-efficacy, and intrinsic interest through proximal self-motivation. *Journal of Personality and Social Psychology, 41*(3), 586-598.

Berg, T., Sharpe, A., & Aitkin, E. (2018). Females in computing: Understanding stereotypes through collaborative picturing. *Computers & Education*, *126*, 105-114.

Blackwell, L. S., Trzesniewski, K. H., & Dweck, C. S. (2007). Implicit theories of intelligence predict achievement across an adolescent transition: A longitudinal study and an intervention. *Child Development*, *78*(1), 246-263.

Blickenstaff, C. J. (2005). Women and science careers: Leaky pipeline or gender filter? *Gender and Education*, *17*(4), 369-386.

Bonsignore, E., Hansen, D., Kraus, K., & Ruppel, M. (2013). Alternate reality games as platforms for practicing 21st-century literacies. *International Journal of Learning and Media*, *4*(1), 25-54.

Bureau of Labor Statistics, U.S. Department of Labor. (2018). *Occupational Outlook Handbook*, Information Security Analysts. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Carpenter, J. (1995). Doctors and nurses: Stereotypes and stereotype change in interprofessional education. *Journal of Interprofessional Care*, *9*(2), 151-161.

Chesler, N. C., Ruis, A. R., Collier, W., Swiecki, Z., Arastoopour, G., & Shaffer, D. W. (2015). A novel paradigm for engineering education: Virtual internships with individualized mentoring and assessment of engineering thinking. *Journal of Biomechanical Engineering*, *137*(2), 024701-024701-8. doi:10.1115/1.4029235

Cheryan, S., Master, A., & Meltzoff, A. N. (2015). Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes. *Frontiers in Psychology*, *6*(49), 1-8. doi: 10.3389/fpsyg.2015.00049

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management* (SAM) (pp. 201-205). The Steering Committee of The

World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Retrieved from https://www.josephpcohen.com/papers/seccomp.pdf

Cohoon, J., & Aspray, W. (Eds.). (2006). *Women and information technology: Research on underrepresentation*. Cambridge, MA: MIT Press.

Dampier, D., Kelly, K., & Carr, K. (2012). *Increasing participation of women in cyber security*. Paper Presented at the ASEE-SE Regional Conference, Starkville, MS.

Diekman, A. B., Brown, E. R., Johnston, A. M., & Clark, E. K. (2010). Seeking congruity between goals and roles: A new look at why women opt out of science, technology, engineering, and mathematics careers. *Psychological Science*, *21*(8), 1051-1057.

Diener, C. I., & Dweck, C. S. (1978). An analysis of learned helplessness: Continuous changes in performance, strategy, and achievement cognitions following failure. *Journal of Personality and Social Psychology*, *36*(5), 451-462.

Diener, C. I., & Dweck, C. S. (1980). An analysis of learned helplessness: II. The processing of success. *Journal of Personality and Social Psychology*, *39*(5), 940-952.

Dweck, C. S. (1975). The role of expectations and attributions in the alleviation of learned helplessness. *Journal of Personality and Social Psychology*, *31*(4), 674-685.

Dweck, C. S. (2008). *Mindset: The new psychology of success.* New York, NY: Random House Digital, Inc.

Dweck, C. S., & Leggett, E. L. (1988). A social-cognitive approach to motivation and personality. *Psychological Review*, *95*(2), 256-273.

Eccles, J. S. (1987). Gender roles and women's achievement-related decisions. *Psychology of Women Quarterly*, *11*(2), 135-172.

Eccles, J. S., Jacobs, J. E., & Harold, R. D. (1990). Gender role stereotypes, expectancy effects, and parents' socialization of gender differences. *Journal of Social Issues*, *46*(2), 183-201.

Ehrlinger, J., Plant, E. A., Hartwig, M. K., Vossen, J. J., Columb, C. J., & Brewer, L. E. (2018). Do gender differences in perceived prototypical computer scientists and engineers contribute to gender gaps in computer science and engineering? *Sex Roles*, *78*(1-2), 40-51.

Frost & Sullivan (2017). *2017 Global information security workforce study: Benchmarking workforce capacity and response to cyber risk.* Center for Cyber Safety and Education, (ISC)2, Booz Allen Hamilton, Alta Associates, and Frost & Sullivan. Retrieved from https://iamcybersafe.org/wpcontent/uploads/2017/03/Womens Report.pdf.

Giboney, J., Hansen, D., McDonald, J., Jonathan, B., Tanner, J., Winters, D., & Bonsignore, E. (2019, January). Theory of Experiential Career Exploration Technology (TECET): Increasing cybersecurity career interest through playable case studies. In *Proceedings of the 52nd Hawaii International Conference on System Sciences.* Retrieved from https://scholarspace.manoa.hawaii.edu/bitstream/10125/59928/1/0488.pdf.

Glaser, B. G. (1965). The constant comparative method of qualitative analysis. *Social Problems*, *12*(4), 436-445.

Hackett, G. (1995). Self-efficacy in career choice and development. In A. Bandura (Ed.), *Self-efficacy in changing societies* (pp. 232-258). New York, NY: Cambridge University Press.

Hansen, D., Bonsignore, E., Ruppel, M., Visconti, A., & Kraus, K. (2013, April). Designing reusable alternate reality games. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1529-1538). ACM. doi. 10.1145/2470654.2466203

Hill, C., Corbett, C., & St. Rose, A. (2010). *Why so few? Women in science, technology, engineering, and mathematics*. Washington, DC: American Association of University Women.

Hulleman, C. S., & Harackiewicz, J. M. (2009). Promoting interest and performance in high school science classes. *Science, 326*(5958), 1410-1412. doi: 10.1126/science.1177067

Jagoda, P., Gilliam, M., McDonald, P., & Russell, C. (2015). Worlding through play: Alternate reality games, large-scale learning, and "The Source." *American Journal of Play*, *8*(1), 74-100.

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I can actually be a super sleuth" Promising practices for engaging adolescent girls in cybersecurity education. *Journal of Educational Computing Research*, *55*(1), 3-25.

Kalwarski, T., Mosher, D., Paskin, J., & Rosato, D. (2007). Best jobs in America [Electronic version]. *CNNMoney. com*. Retrieved February 20, 2007. Retrieved from http://money.cnn.com/magazines/moneymag/bestjobs/ index.html

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology, 77*(6), 1121-1134.

Linnenbrink-Garcia, L., Perez, T., Barger, M. M., Wormington, S. V., Godin, E., Snyder, K. E., ... & Schwartz-Bloom, R. (2018). Repairing the leaky pipeline: A motivationally

supportive intervention to enhance persistence in undergraduate science pathways. *Contemporary Educational Psychology*, *53*, 181-195.

Margolis, J., & Fisher, A. (2003). *Unlocking the clubhouse: Women in computing.* Cambridge, MA: MIT press.

Master, A., Cheryan, S., & Meltzoff, A. N. (2016). Computing whether she belongs: Stereotypes undermine girls' interest and sense of belonging in computer science. *Journal of Educational Psychology*, *108*(3), 424-437.

McDonald, J. K., Hansen, D. L., Balzotti, J., Johnson, T., Winters, D. M., Giboney, J., Bonsignore, E. (2019, January). *Designing authentic cybersecurity experiences: Lessons from the Cybermatics playable case study.* Paper presented at the 52nd Hawaii International Conference on System Sciences (HICSS), Maui, HI.

Morgan, S. L., Gelbgiser, D., & Weeden, K. A. (2013). Feeding the pipeline: Gender, occupational plans, and college major selection. *Social Science Research, 42*(4), 989-1005.

National Science Board. (2016). *Science and Engineering Indicators 2016*. Alexandria, VA: National Science Foundation (NSB-2016-1). Retrieved from https://www.nsf.gov/statistics/2016/nsb20161/uploads/1/12/chapter-2.pdf

National Science Foundation, National Center for Science and Engineering Statistics. (2017). *Women, Minorities, and Persons with Disabilities in Science and Engineering: 2017.* Special Report NSF 17-310. Arlington, VA. Retrieved from at www.nsf.gov/statistics/wmpd/

Niemeyer, G., Garcia, A., & Naima, R. (2009, October). Black cloud: Patterns towards da future. In *Proceedings of the 17th ACM International Conference on Multimedia, Beijing, China*, (pp. 1073-1082). New York, NY: ACM. doi:10.1145/1631272.1631514

Oakes, J., & The RAND Corporation. (1990). Opportunities, achievement, and choice: Women and minority students in science and mathematics. *Review of Research in Education, 16,* 153-222. doi: 10.2307/1167352

Paris, L. D., & Decker, D. L. (2012). Sex role stereotypes: Does business education make a difference? *Gender in Management: An International Journal*, *27*(1), 36-50.

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology, 9*(1), 25-44.

Pell, A. N. (1996). Fixing the leaky pipeline: Women scientists in academia. *Journal of Animal Science*, *74*(11), 2843-2848.

Pintrich, P. R., & De Groot, E. V. (1990). Motivational and self-regulated learning components of classroom academic performance. *Journal of Educational Psychology, 82*(1), 33-40.

Ryan, C., & Lewis, J. (2017). *Computer and Internet Use in the United States: 2015- American Community Survey Reports* (Report No. ACS-37). Retrieved from U.S. Department of Commerce Economics and Statistics Administration website: https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf

Sadker, M., & Sadker, D. (2010). *Failing at fairness: How America's schools cheat girls*. New York, NY: Simon and Schuster.

Schott, G., & Selwyn, N. (2000). Examining the "male, antisocial" stereotype of high computer users. *Journal of Educational Computing Research*, *23*(3), 291-303.

Schunk, D. H. (1982). Progress self-monitoring: Effects on children's self-efficacy and achievement. *The Journal of Experimental Education*, *51*(2), 89-93.

Schunk, D. H. (1991). Self-efficacy and academic motivation. *Educational Psychologist*, *26*(3-4), 207-231.

Schunk, D. H., Hanson, A. R., & Cox, P. D. (1987). Peer-model attributes and children's achievement behaviors. *Journal of Educational Psychology, 79*(1), 54-61.

Schunk, D. H. & Zimmerman, B. J. (2007) Influencing children's self-efficacy and self-regulation of reading and writing through modeling. *Reading & Writing Quarterly*, *23*(1), 7-25. doi: 10.1080/10573560600837578

Shaffer, D. W. (2006). Epistemic frames for epistemic games. *Computers & Education, 46*(3), 223-234.

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., ... & Hall, L. (2013, June). Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE Working Group Reports Conference on Innovation and Technology in Computer Science Education-Working Group Reports, Canterbury, England, UK*, (pp. 1-14). New York, NY: ACM. doi: 10.1145/2543882.2543883

Steele, C. M. (1997). A threat in the air: How stereotypes shape intellectual identity and performance. *American Psychologist, 52*(6), 613-629.

Taylor, E., & Antony, J. S. (2000). Stereotype threat reduction and wise schooling: Towards the successful socialization of African American doctoral students in education. *Journal of Negro Education*, *69*(3), 184-198.

Thom, M., Pickering, M., & Thompson, R. E. (2002). Understanding the barriers to recruiting women in engineering and technology programs. In *Proceedings of the 32nd ASEE/IEEE Frontiers in Education Conference* (pp. 1-6). Boston, MA: ASEE. Retrieved from file:///Users/desireewinters/Downloads/understanding-the-barriers-to-recruiting-women-in-engineering-and-technology.pdf

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads, 5*(1), 53-56.

Wynn, A. T., & Correll, S. J. (2018). Puncturing the pipeline: Do technology companies alienate women in recruiting sessions? *Social Studies of Science*, *48*(1), 149-164.

Zimmerman, B. J. (1995). Self-efficacy and educational development. In A. Bandura (Ed.), *Self-efficacy in changing societies* (pp. 202-231). New York, NY: Cambridge University Press.

Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. *Contemporary Educational Psychology, 25*(1), 82-91.

APPENDIX A

IRB Approval Letter

Institutional Review Board
for Human Subjects

Brigham Young University
A-285 ASB Provo, Utah 84602
(801) 422-3841 / Fax: (801) 422-0620

October 25, 2016

Professor Derek Hansen
A-285 ASB
Campus Mail

Re: Improving Argumentative Writing through Playable Case Studies

Dear Professor Derek Hansen

This is to inform you that Brigham Young University's IRB has approved the above research study.

The approval period is from 10-25-2016 to 10-24-2017. Your study number is E16364. Please be sure to reference this number in any correspondence with the IRB.

Continued approval is conditional upon your compliance with the following requirements.

1. A copy of the 'Informed Consent Document' approved as of 10-25-2016 is enclosed. No other consent form should be used. It must be signed by each subject prior to initiation of any protocol procedures. In addition, each subject must be given a copy of the signed consent form.

2. All protocol amendments and changes to approved research must be submitted to the IRB and not be implemented until approved by the IRB.

3. The enclosed recruitment advertisement has been approved. Advertisements, letters, Internet postings and any other media for subject recruitment must be submitted to IRB and approved prior to use.

4. A few months before this date we will send out a continuing review form. There will only be two reminders. Please fill this form out in a timely manner to ensure that there is not a lapse in your approval.

If you have any questions, please do not hesitate to call me.

Sincerely,

Robert Ridge, PhD, Chair
Sandee Aina, MPA, Administrator
Institutional Review Board for Human Subjects

INSTITUTIONAL REVIEW BOARD
FOR HUMAN SUBJECTS

Memorandum

To: Professor Derek Hansen
Department: TECH
College: E&T
From: Sandee Aina, MPA, IRB Administrator
Bob Ridge, PhD, IRB Chair
IRB#: E16364
Title: *"Improving Argumentative Writing through Playable Case Studies"*

Brigham Young University's IRB has renewed its approval of the research study referenced in the subject heading. The amendment submitted with the renewal materials has also been approved. The approval period is from **October 22, 2018 to October 24, 2019**. All conditions for continued approval during the prior approval period remain in effect. These include, but are not necessarily limited to the following requirements:

1. A copy of the consent forms are attached to this email. No other forms should be used. Each research subject must sign the form prior to initiation of any protocol procedures. In addition, each subject must be given a copy of the signed consent form.
2. Any modifications to the approved protocol must be submitted, reviewed, and approved by the IRB before modifications are incorporated in the study.
3. In addition, serious adverse events must be reported to the IRB immediately, with a written report by the PI within 24 hours of the PI's becoming aware of the event. Serious adverse events are (1) death of a research participant; or (2) serious injury to a research participant.
4. All other non-serious unanticipated problems should be reported to the IRB within 2 weeks of the first awareness of the problem by the PI. Prompt reporting is important, as unanticipated problems often require some modification of study procedures, protocols, and/or informed consent processes. Such modifications require the review and approval of the IRB.

IRB Secretary
A 285 ASB
Brigham Young University
(801)422-3606

APPENDIX B

IRB Parental Consent Form

Parental Permission for a Minor

Introduction

This research is conducted by Dr. Derek Hansen and other faculty and graduate students at Brigham Yount University and the University of Maryland. The goal is to develop and improve interactive, educational simulations. Your child's teacher will be using one of our simulations in class. We are inviting your child to take part in the research about its effectiveness.

Procedures

If you agree to let your child participate in this research study, your child will complete the simulation during their regular class with no interruption to their regular school schedule. Permission will also grant access to the collection of data (i.e. assignment and assessment scores regarding the simulation and audio recordings of class sessions and interviews). As a part of the class, your student may be asked to participate in a series of interviews, surveys, and observations during the semester that he or she is enrolled in this class. These interviews will ask him or her to talk about his or her attitudes about the simulation and about online simulations generally. Data will be collected from these interviews, surveys, and observations.

Risks

The risks of this study are minimal. Answering interview questions should not require students to disclose sensitive or personal information, and your child will be free to refuse to answer any question. There is a risk of loss of privacy, which we will reduce by not using any real names or other identifiers in publications. Data will be secured as described below.

Confidentiality

The research data will be kept on password-protected computers and only the researchers will have access to the data. At the conclusion of the study, all identifying information will be removed and the data will be kept in a locked cabinet or office. The information and data collected from this study will be stored on a password-protected computer for up to five years after the study is finished and then destroyed to ensure confidentiality.

Benefits

There are no direct benefits for your child's participation in this project. However, teachers, educators and researchers will benefit from potential understandings about how to maximize the potential of teaching and learning simulations in ways that will enhance students' engagement and sense of identity.

Compensation

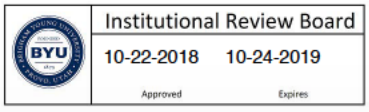
There will be no compensation for participation in this project.

Questions about the Research

Please direct any further questions about the study to Derek Hansen (801) 422-7467 or dlhansen@byu.edu.

Questions about your child's rights as a study participant or to submit comment or complaints about the study should be directed to the IRB Administrator, Brigham Young University, A-285 ASB, Provo, UT 84602. Call (801) 422-1461 or send emails to irb@byu.edu.

You have been given a copy of this consent form to keep.

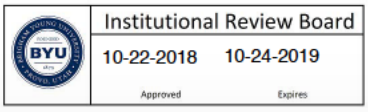


Participation

Participation in this research study is voluntary. You are free to decline to have your child participate in this research study. You may withdraw you child's participation at any point without affecting your child's grade or standing in this class.

Child's Name: _____

Parent Name: _____ Signature: _____ Date: _____



APPENDIX C

IRB Child Assent Form

Child Assent

What is this research about?

As a research group at Brigham Young University and the University of Maryland, we would like to invite you to take part in a research study. We are trying to learn more about online simulations to help introduce students to new topics and/or learn new skills.

What will I be asked to do?

If you decide to be a part of this study, here's what will happen. The curriculum of this course will be presented in your regular high school class. Your participation will take place during your normal class time and under the guidance of your teacher; however, if you wish to participate in this study, the results of your assignments will be gathered to analyze whether using interactive, online simulations are beneficial. All the data that we will collect, including your responses and audio recordings of class sessions and interviews, will be stored securely and confidentially. Only those participating in the research will be able to view your writing or listen to the audio recordings, so your work and identity will remain private. Finally, the research team will be observing the class throughout the semester. As we take notes and document what occurs in the class, we will be noting your participation. These observations will be recorded as notes we take on our computers.

Can anything bad happen to me?

It is unlikely that anything bad will happen to you if you participate. Only the researchers will have access to the data collected. The information collected from this study will be stored on password-protected computers and destroyed five years after the study is finished.

Can anything good happen to me?

We don't know if being in this study will help you, but we hope to learn things that will help other students and teachers.

Do I have other choices?

You can choose not to be in this study. If you choose not to be in the study, you will be expected to complete the simulation as course work; however, your data will not be collected for observation.

Will anyone know I am in the study?

We won't tell anybody that you are in this study. Your parent or guardian may know that you took part in the study. When we tell other people or write articles about what we learned in the study, we won't include your name or the name of anyone else who took part in the study.

What happens if I get hurt?

Your parent or guardian will have more information on a separate form, and if you are uncomfortable with anything that happens as a result of this study, you can talk to them or a member of the research team.

What if I do not want to do this?

You don't have to be in this study. It's up to you. If you say yes now, but change your mind later, that's okay too. All you have to do is tell us. You will not receive any kind of reward (money, extra credit, etc.) for being in this research study. Before you say yes to be in this study, be sure to ask one of us to tell you more about anything that you don't understand.

If you want to be in this study, please sign and print your name.

Name (Printed): _____ Signature _____ Date: _____

Ages 7-14

APPENDIX D

Pre-Simulation Survey Questions

Self-efficacy

The following questions were presented on a 7-point Likert scale (1 = not at all true of me to 7 = very true of me), adapted from the Motivated Strategies for Learning Questionnaire (Pintrich, & De Groot, 1990):

1. I expect that I could do very well in a cybersecurity class.
2. I am sure I could do an excellent job on the problems and tasks assigned in a cybersecurity class.
3. I'm certain that I can understand the ideas taught in a cybersecurity course.
4. I think I would receive a good grade in a cybersecurity class.
5. I know that I will be able to learn the material taught in a cybersecurity class.

Interest

The following questions were presented on the same 7-point Likert scale)

1. I am interested in cybersecurity
2. I would like to learn more about cybersecurity.
3. I plan on taking a cybersecurity class in the future.

Miscellaneous

1. What skills do you believe are most important for a cybersecurity professional have?

APPENDIX E

Additional Post-Simulation Survey Questions

The post-simulation survey included the questions on the pre-simulation survey, along with several additional questions, including:

1. What did you like most about your time at Cybermatics?
2. What could Cybermatics do to improve the experience for new hires like you?
3. What did you learn from your time at Cybermatics?
4. How have your perceptions about cybersecurity changed as a result of your time at Cybermatics?
5. Do you feel that your time at Cybermatics increased your confidence in your ability to do well in a cybersecurity class in the future?

The post simulation also included the following questions on a 7-point Likert scale:

1. I was able to complete the tasks assigned to me at Cybermatics effectively.
2. I enjoyed my time at Cybermatics

APPENDIX F

Focus Group and Interview Prompts

1. Tell me about your experience with Cybermatics.
    a. What did you like about the simulation?
    b. What didn't you like about the simulation?
2. Tell me about your process of working through hard parts of the simulation.
3. What did you know about cybersecurity before your experience with the Cybermatics PCS?
4. How do you think your perceptions about cybersecurity have changed?
5. Do you think the simulation made you more or less interested in learning about cybersecurity?
6. Before the simulation, would you have thought you could be good at cybersecurity?
7. Do you think the simulation helped you feel more confident that you could be successful if you took a class in cybersecurity?