TechTrends (2021) 65:496–510
https://doi.org/10.1007/s11528-021-00585-w

ORIGINAL PAPER

Increasing Cybersecurity Career Interest through Playable Case Studies

Justin Scott Giboney[1] · Jason K. McDonald[1] · Jonathan Balzotti[1] · Derek L. Hansen[1] · Desiree M. Winters[1] · Elizabeth Bonsignore[2]

Accepted: 19 January 2021 / Published online: 8 February 2021

Abstract
In this paper we introduce an approach to cybersecurity education and helping students develop professional understanding in the form of a Playable Case Study (PCS), a form of educational simulation that draws on affordances of the broader educational simulation genre, case study instruction, and educational Alternate Reality Games (or ARGs). A PCS is an interactive simulation that allows students to "play" through an authentic scenario (case study) as a member of a professional team. We report our findings over a multi-year study of a PCS called Cybermatics, with data from 111 students from two different U.S. universities who interacted with the PCS. Cybermatics increased student understanding about certain key aspects of professional cybersecurity work, improved their confidence in being able to successfully apply certain skills associated with cybersecurity, and increased about half of the students' interest in pursuing a cybersecurity career. Students also reported a number of reasons why their perceptions changed in these areas (both positive and negative). We also discuss design tensions we experienced in our process that might be encountered by others when creating simulations like a PCS, as they attempt to balance the authenticity of designed learning experiences while also sufficiently scaffolding them for newcomers who have little background in a discipline.

Keywords Educational simulations · Career exploration · Alternate reality games · Playable case studies · Instructional design principles

An estimated 1.8 million cybersecurity positions will be unfilled by 2022 (Center for Cyber Safety Education, (ISC)2, Booz Allen Hamilton et al. 2017), and an increasing number of other technical jobs will demand some type of cybersecurity knowledge (Kay et al. 2012). Yet despite high salaries and opportunities, there is a lack of awareness of cybersecurity education and job opportunities among students who are choosing college majors and careers (Baker 2016; Shumba et al. 2013; Vogel 2016). Even students that are aware of cybersecurity jobs report a lack of understanding of the nature of the associated job tasks (Raytheon 2016) and cybersecurity professionals report significant misperceptions among prospective women employees (LeClair and Pheils 2016).

✉ Jason K. McDonald
jason@byu.edu

[1] Brigham Young University, 150-E MCKB, Provo, UT 84602, USA

[2] University of Maryland, College Park, MD, USA

To address these concerns, in this paper we introduce an approach to cybersecurity education, including helping students develop professional understanding of the field, in the form of a Playable Case Study (PCS), a form of educational simulation that draws on affordances of the broader educational simulation genre (Gredler 2004), case study instruction (Heitzmann 2008), and educational Alternate Reality Games or ARGs (Battles et al. 2011; Jagoda et al. 2015; Johnston et al. 2012; Niemeyer et al. 2009). Specifically, a PCS is an interactive simulation that allows students to "play" through an authentic scenario (case study) as a member of a professional team. Participants advance the storyline as they complete professional tasks and communicate with fictional characters through a realistic transmedia interface (Hansen et al. 2017). A PCS provides an authentic professional experience (albeit simulated), along with a safe place for students to fail as they learn. They are also highly scalable, since they do not require significant technical setup or knowledge by the instructors.

We illustrate the PCS concept through research on a cybersecurity-focused PCS, Cybermatics, that allows college students to work alongside fictional characters on a realistic

cybersecurity engagement. Cybermatics was developed and tested in a university setting, in collaboration with academics from two universities. Our goal in introducing Cybermatics is to present evidence of the effects this form of education intervention can have on student learning, describe challenges and opportunities afforded by the PCS genre, and provide design recommendations to others designing similar immersive educational experiences. Specifically, we address the question: what effects does the Cybermatics PCS have to help students

a) Better understand what skills and traits are needed for cybersecurity professionals;
b) Increase confidence in their ability to succeed in a cybersecurity career; and
c) Increase their interest in pursuing a career in cybersecurity?

Our paper is structured as follows: we first describe a growing interest in developing novel educational interventions within cybersecurity education contexts, as well as limitations of current approaches. We then describe the Cybermatics PCS, summarizing work performed throughout the past four years as we have developed, iteratively improved, and systematically studied it in classes at two universities (Giboney et al. 2019; McDonald et al. 2019). Our report on data collected from multiple universities and classrooms shows how students learn from a PCS, and how it can help increase their interest in cybersecurity. We finally provide a discussion of our findings to help future designers of educational simulations increase their effectiveness.

Literature Review

Cybersecurity Competitions and Camps

A growing body of literature has examined interventions designed to raise awareness and understanding of cybersecurity content and jobs, though there is significant room for improvement. Researchers have focused their attention on curriculum development in cybersecurity education (Bustos 2017; McGettrick et al. 2014; Raj and Parrish 2018; Shackelford et al. 2015; Yang and Wen 2017), as well as training/awareness programs for the field (Adams and Makramalla 2015; Gavas and Memon 2012; Giannakas et al. 2015; Nagarajan et al. 2012). Two of the more engaging and common of these interventions have been cybersecurity competitions and cybersecurity camps. While each has helped raise awareness of cybersecurity, they can also be problematic as both recruitment and educational tools.

Cybersecurity competitions are a common and highly visible technique for raising awareness of cybersecurity, as well as identifying talent and motivating learning. Popular competitions are sponsored by government and industry. Examples include CyberPatriot, the National Cyber League, DEF CON Contests, the National Collegiate Cyber Defense Competition, and numerous Capture the Flag competitions. On the positive side, competitions are highly engaging and use experiential and problem-based learning techniques that can be applied in real-world contexts (Katsantonis et al. 2017). This is likely why they have been shown to increase student interest in cybersecurity (Cheung et al. 2012; Werther et al. 2011) and are recommended as an important component of the cybersecurity outreach and training efforts (McGettrick et al. 2014).

Unfortunately, there are also many factors that make cybersecurity competitions less than ideal as a recruitment and educational tool. Competitions can require significant time and technical resources to implement, require expert support personnel, have high quality assurance standards to make sure they are "fair," and happen infrequently or at fixed times that may not work for certain learners (Cheung et al. 2012; Katsantonis et al. 2017). Competitions are better suited for measuring (i.e., evaluating) existing skills than developing new skills (Cheung et al. 2012), fail to address the day-to-day context and management of cybersecurity in realistic ways, are not calibrated to participants' needs (e.g., do not include personalized educational scaffolding), do not support partial credit, and do not provide an experimental environment where students can safely fail, revise, improve, and succeed (Katsantonis et al. 2017). They are also considered extracurricular activities in most cases, limiting their potential reach in formal education settings (Cheung et al. 2012). Partly due to self-selection, competitions are best suited for reinforcing the interests of those with relatively-high levels of cybersecurity skills, not teaching concepts or recruiting those who do not already know they want to go into the field (Tobey et al. 2014). Thus, cybersecurity competitions are most useful in attracting those with some prior experience, or who already have some degree of self-efficacy concerning a cybersecurity career (Bashir et al. 2017).

Another common approach is to run cybersecurity camps or after-school clubs such as GenCyber, CybHER, or camps held at universities. Camps often include hands-on experiential learning activities, as well as discussions about careers in cybersecurity (Jethwani et al. 2017; Rowland et al. 2018; Tims et al. 2014). Some are tied to highly engaging game-like experiences, such as the starship simulator with embedded cybersecurity activities (C. Cornel et al. 2016; C. J. Cornel et al. 2017). These and related experiences at camps can help students feel excitement about cybersecurity, as well as gain exposure to core concepts and mindsets (Rowland et al. 2018). They have been shown to improve the perceived value of cybersecurity among women, along with positively impacting their cyber self-efficacy (Tims et al. 2014). Cybersecurity camps, in contrast to strictly computer science and coding focused camps, appeal more to female students with their focus on collaboration, communication (e.g., secret messages), creative problem solving, and real-world and pro-social topics (e.g., catching bad guys through forensics; crisis response) (Jethwani et al. 2017; Tims et al. 2014).

Unfortunately, camps are typically short extracurricular experiences designed for those who already have interests in cybersecurity and can afford them. Camps also take considerable funding and resources to run, including development of hands-on learning experiences, finding instructors with expertise, travel, and the logistics of food and lodging.

To attract an increasing number and more diverse student group to cybersecurity careers, it is essential that interventions be developed that leverage the strengths of competitions and camps, while also overcoming some of their inherent limitations. Research suggests that interventions that build confidence (i.e., self-efficacy), use active learning, and help students identify as a STEM professional are needed to increase persistence in STEM majors (Graham et al. 2013). While such experiences will share much with the highly engaging, experiential learning focus of competitions and camps, they will have a larger impact if they (a) integrate into formal classroom environments, thus reaching new potential students; (b) simplify the setting up of technical infrastructure; (c) lower the inherent risks associated with non-experts conducting cybersecurity activities; (d) be more scalable across time and distance; (e) require less expertise by those who manage and run them; (f) provide a professional context in which cybersecurity work happens; and (g) provide sufficient educational scaffolding so task completion is attainable for all participants, regardless of background experience.

Simulated Professional Practice

For professional fields, educational simulations and other forms of digital experiential learning have been identified as means of encouraging a sense of reflective practice, meaning they can help students (as potential professionals) draw a connection between knowing and doing (Shaffer 2005). The design processes used to create such experiences have been identified by Shaffer (2004) as a theory of pedagogical praxis, arguing that "under the right conditions, computers and other information technologies can make it easier for students to become active participants in meaningful. .. practices of life" (p. 1401). The value of praxis-focused approaches provides simulated forms of professional life (Chesler et al. 2015) that teach students ways of thinking and acting modeled on professional practice. Teaching disciplinary skills in the context of the professional environments in which they are commonly used improves students' views of how valuable those skills are, because students report seeing those skills as a way to accomplish important, real-world goals (Schank 1994).

Alternate Reality Games

Creating more authentic learning environments and realistic contexts that are still engaging to students can be challenging. A key inspiration for the development of the PCS more generally (Hansen et al. 2017), and Cybermatics specifically, is a new genre of transmedia storytelling called alternate reality games (ARGs). ARGs allow players to solve puzzles and interact with fictional characters to further a story that is told using everyday technologies, such as email, videoconferencing, websites, etc. (Pellicone et al. 2017). A key design principle of ARGs is the philosophy of This is Not a Game (TINAG) (Flushman et al. 2015). TINAG means the simulation or game strives to help participants perceive that the simulation is occurring in real life. Instead of relying on artificial mechanisms of advancing the game's story like cards, dice, or controlling an avatar on a screen, ARGs and PCSs that comply with TINAG have players advance the story through the use of everyday actions and technologies. For example, instead of players reading "out-of-game" instructions on how to use a website, a game character would introduce how to use the website in an authentic "in-game" manner (e.g., your fictional supervisor shows you how to use the website since you are a new hire). TINAG can help students better understand and make connections between the skills, knowledge, identity, dispositions, values, and epistemology unique to that profession (Bonsignore et al. 2013; Shaffer 2005).

Cybermatics: A Playable Case Study

Consistent with the principles of simulating professional practice as well as for developing ARG environments, we designed a playable case study called Cybermatics with three objectives. The first objective was to help students better understand what knowledge, skills, and traits are needed for cybersecurity professionals. Students that better understand the job will be able to better decide whether a career in cybersecurity is right for them. Our second objective was to help increase students' interest in cybersecurity as a potential career. Our final objective was to help students increase their confidence in their ability to succeed in a career in cybersecurity.

Cybermatics is designed for integration into a formal classroom environment. Many of the skills, knowledge, and dispositions the PCS aims to help students develop correlate with key learning outcomes, making its use in classroom contexts justifiable from an educational perspective. Furthermore, teachers can both leverage the PCS activities to springboard classroom discussion and tailor classroom discussion to scaffold the PCS tasks. While the PCS was designed for students to complete individually, students can ask an instructor for help, and many instructors used simulation activities to begin in-class discussions of key concepts. Prior to the simulation, students should have learned relevant topics in class such as databases (e.g., SQL) and have received at least a high-level overview of computer security.

Cybermatics gives students a "week-in-the-life," simulated experience of a professional penetration tester (pentester). As

students log into the online simulation, they adopt the role of a newly hired employee in a cybersecurity company called Cybermatics, right before the company starts a penetration test for a fictional home automation company called Riptech. The player learns cybersecurity terminology and completes tasks (such as SQL injection and password cracking) with the help of virtual team members. As the simulated timeline advances, a storyline develops in which the security team discovers that a rogue Riptech employee has entered backdoor code into the Riptech system in order to obtain access to customer data. The student does some virtual sleuthing on the RipTech Linux server and, with the aid of virtual team members, discovers the file to the backdoor code. This discovery is reported to the team, and then to the Riptech CEO. The simulation ends with a video of the Riptech employee being arrested, after which each student submits a final penetration testing report to Riptech's CEO.

This narrative unfolds over the course of five simulated "days," each of which must be completed in order to advance to the next (Table 1). Assignments, cybersecurity tools, and educational scaffolding are integrated into the online simulation and supplemented by in-class discussions and lesson plans. The simulated days do not correspond to days in the real-world; in actuality, the simulation comprises 4–6 class periods spread out over two weeks (about six hours of class time), with another few hours devoted to homework assignments.

Within the simulation, the project manager, Kimberly, assigns students to tasks for each of the simulation days. Once completed, students click a "Next Day" button, which triggers the release of new content, including new tasks, group chat messages, video conference calls, and documents (Fig. 1). Students interact with other Cybermatics team members who share their own findings, give advice, and model positive and negative behaviors. Kimberly also praises positive behaviors and identifies and appropriately addresses the negative behaviors. Communication with Kimberly and other characters (team members) occurs through a realistic, yet simplified interface modeled after a corporate intranet. It includes a group chat system that uses a chat-bot to dynamically respond to player input from different fictional characters.

The interface is modeled after a corporate Intranet. Cybersecurity tools and aids are accessible, most prominently in the form of a Terminal interface (a custom simulated shell) that allows students to run Linux commands to perform various tasks (Fig. 2). Educational scaffolding is incorporated through character chat messages, videoconferencing, and Cybermatics internal documentation on topics relevant to the simulation (Fig. 3). The goal of the interface is to be as authentic as possible, while also simplifying the representations and allowing students to easily track their progress.

All material, including an introductory email describing the intranet features, are presented in an "in game" manner consistent with the principle of TINAG described earlier. For example, the introductory email is not from an educator introducing the simulation, it is from a human resources Cybermatics employee welcoming students to the company. Players also complete in game assessments, in the form of performing a penetration test on the Riptech website, which looks like an authentic home automation company website (Fig. 4). Student players regularly add sections to the final penetration testing report throughout the experience in order to help them reflect on what was accomplished each day (Fig. 5).

Method

We have studied the effects of Cybermatics over the past four years using principles inspired by design science research, a methodology for identifying features of technology to build grounded theories about its operation, optimization, and/or outcomes from a technological and/or behavioral perspective (Hevner et al. 2004; Nunamaker Jr. and Briggs 2011; Peffers et al. 2007). In summary, our methodological procedures were

Table 1 Cybermatics Narrative

Day	Narrative	Goals
1	Introduce the team, the scope, the target company RipTech, and the RipTech CEO.	Students learn the concept of ethical penetration testing and how to navigate the simulation.
2	Visit RipTech.io website. Receive instructions for and start the penetration test. A coworker gets in trouble for violating scope.	Learn about SQL injection and technical report writing. Obtain usernames and password hashes using SQL injection.
3	Look at evidence of a bad actor gathered by a coworker who social engineers his way into the RipTech offices. Use a password to further penetrate the company.	Learn how to crack password hashes in a shell environment.
4	Explore the target company server using remote access. Find more evidence of a backdoor from the bad actor and report it to the CEO who contacts the FBI.	SSH into the target company. Learn more about Linux. Find evidence of bad actor on server files.
5	End the simulation. FBI arrests the bad actor. Write up your sections of the penetration testing report.	Learn how to write up a penetration testing report.

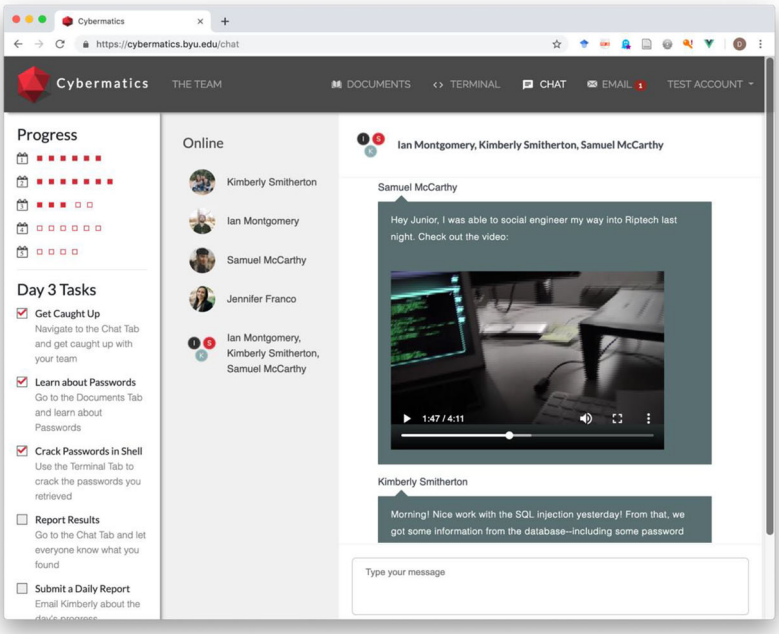

Fig. 1 Sample Cybermatics Interface

to: (a) identify an educational problem to explore; (b) define the objectives of a solution; (c) design and develop an educational technology artifact as a possible implementation of our solution criteria; (d) demonstrate the use of the artifact; (e) evaluate the potential value of the artifact; and (f) communicate the design and significance of the artifact and findings (Peffers et al. 2007). We have already described the problem, the objectives, and the design of the artifact in our discussion of Cybermatics above. In this section, we describe our research and evaluation methodology. Following sections will report the findings from our study, which demonstrate the use of the Cybermatics artifact, its potential, and significance.

We used a mixed-methods approach to evaluate the Cybermatics PCS including a pre- and post-survey, classroom observation, digital trace data, and written student feedback about the experience. Data was collected and analyzed from 132 students in introductory courses from two universities in different parts of the United States. 21 students did not complete the interaction or failed attention checks in the survey. Of the remaining 111 students, 77 (69.4%) identified their gender as male, 31 (27.9%) identified their gender as female, and 3 did not identify. The average age of the 111 students was 20.42 with a standard deviation of 2.83. One class was an introductory Information Technology (IT) class, primarily consisting of IT majors, though it also included students from ancillary majors exploring IT. Many of these students have an interest in Cybersecurity, which is a major emphasis area within the IT program. The other class was an undergraduate

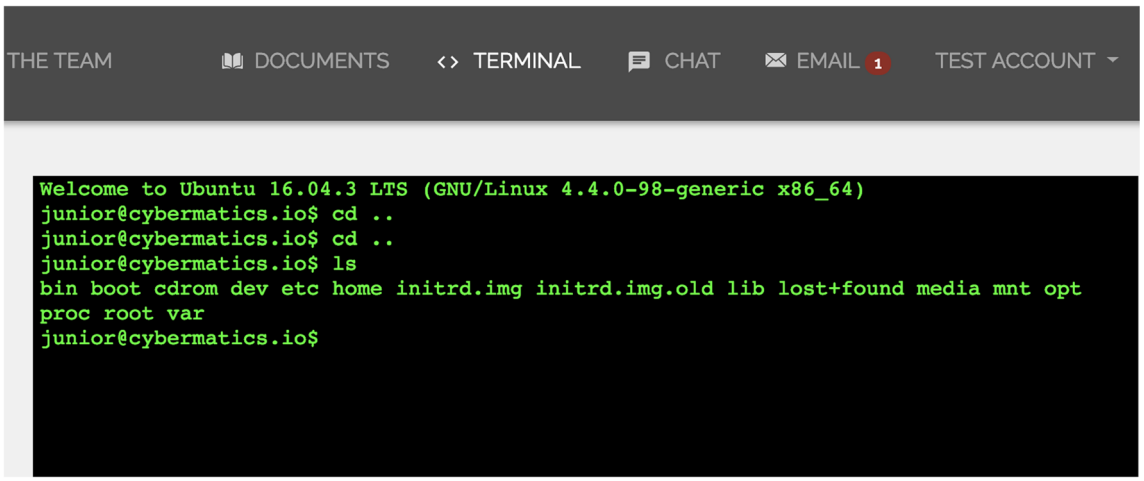

Fig. 2 Cybermatics Terminal Interface

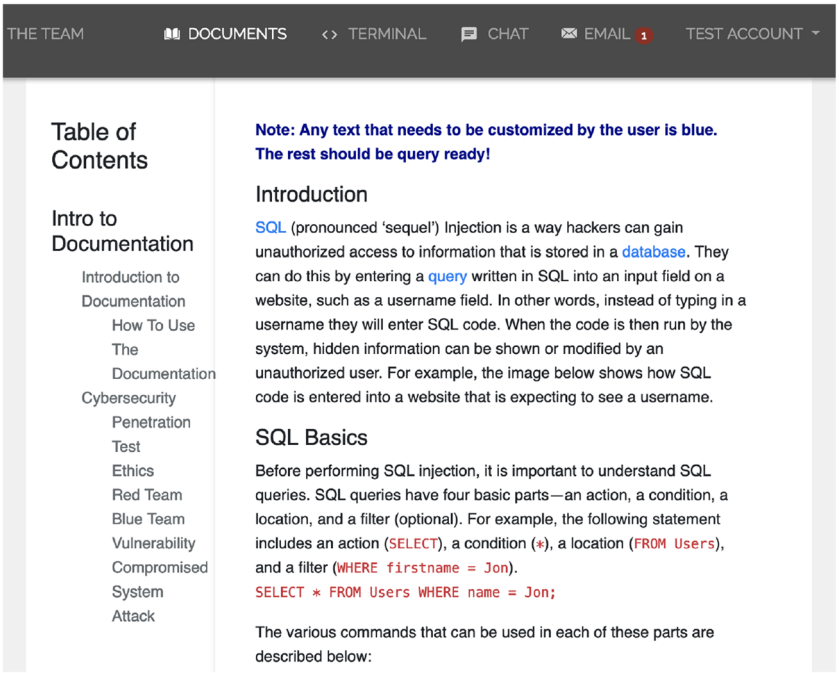

Fig. 3 Cybermatics SQL Injection Documentation

introduction to Information Science course for students in, or exploring, the major. Fewer of these students focus on Cybersecurity, though it is a topic of interest to some. While some students did enter these classes with a general interest in Cybersecurity, only 14% described any prior instruction or training in the topic, and in the majority of those cases they reported their prior knowledge as being minimal. However, 88.8% of students had taken other Information Technology courses that required them to learn some programming/coding, which was background knowledge that would be useful for the simulation. Both teachers were using the Cybermatics PCS for the first time and were not part of the design team, although a TA and members of the design team were available to help in the IT class at one of the locations.

We asked students a series of questions before and after their interactions with the simulation. After IRB statements, in a presurvey we measured the students' interest in cybersecurity using a sliding bar from 0 to 100 related to agreement with the following three statements: (a) I am interested in cybersecurity; (b) I plan on pursuing a career in cybersecurity; and (c)

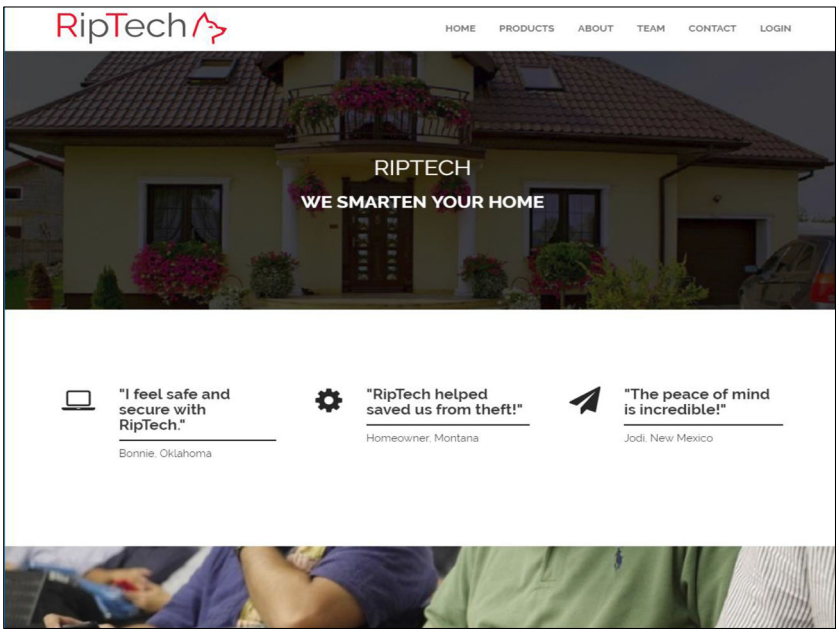

Fig. 4 Target Fictitious Company Website for Cybermatics Penetration Test

Fig. 5 Sample Report Template that Students Modify

RIPTECH PENETRATION TEST FINAL REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Scope of Work

Cybermatics completed a penetration test on the systems from Riptech LLC, in accordance with the agreed scope document conditions. The test included all forms of cyber attack targeting the RipTech website, as well as a physical attack that included only social engineering techniques; breaking and entering the premises was disallowed.

Project Objectives

- Gain remote access to Riptech servers.
- Escalate privileges to attempt to gain admin access to Riptech's databases.
- Explore the available databases using admin rights to find any insecure information.
- Use social engineering to test Riptech's employees' compliance with safety protocol.

Summary of Findings

Provide a list of the key problems that were identified

I feel confident in my ability to succeed in the cybersecurity field. We also measured students' perception of the importance of eight skills to cybersecurity professionals and, in separate questions, students' confidence in their own abilities to the same eight skills: leadership, communication, adaptability, problem solving, ethics, programming, ability to learn on their own, and attention to detail. We asked the same two questions to elicit responses on these eight skills in the post survey, to measure effects of the PCS on students' responses. In the post survey, we also asked students to respond to three, 7-point Likert scale items about how the PCS changed their view of a career in cybersecurity:

- The simulation made me more likely to pursue a career in cybersecurity.
- The simulation made me more confident in my ability to succeed in a cybersecurity career.
- I would recommend the simulation to people deciding whether to pursue a career in cybersecurity.

The survey also included two questions to elicit qualitative responses:

- How have your perceptions about cybersecurity changed after completing the simulation?
- If you are not interested in cybersecurity, please list 3–5 reasons why you are not interested.

Other questions in the post survey focused on what students liked and disliked about the design of the simulation. Researchers took notes on observations during the IT class lab sessions where students worked on the PCS. These included notes on difficulties students encountered, comments they made to each other, and reactions to the narrative. The Information Science class students also provided written notes about their experience with the simulation. Qualitative data was analyzed by the team using a thematic analysis process that first, identified common themes related to student perceptions of the simulation, and second, identified the design

elements of the PCS that students described helped or hindered them in achieving the goals of the PCS.

Findings

Quantitative Results

For questions measured in both the pre- and post-surveys we ran a paired T-test to look for effects of the PCS. We used a Holm-Bonferroni correction because of the number of T-tests that we performed (Holm 1979). Figure 6 shows the self-reported impact of the simulation on students. 47.2% of students agreed at some level that they were more likely to pursue a career in cybersecurity after the simulation, with males being significantly more likely (p = 0.037). 50.9% of students agreed at some level that they were more likely to succeed in a cybersecurity career as a result of the simulation, with males again being significantly more likely (p = 0.016). 68.5% of students agreed at some level that they would recommend the simulation to others trying to decide on a career in cybersecurity (with no difference in gender). While we cannot conclude there is a causal relationship between completing the PCS and these self-reports, we are encouraged that so many students responded positively to these key issues immediately following their experience with the simulation.

Table 2 reports differences between the pre- and post-survey questions. Note that using a Holm-Bonferroni correction means that only the two T values greater than 4 are significant. This correction indicates that the other significant results could have been due to chance. Students' understanding of what penetration testers do increased dramatically, suggesting that they had limited understanding of the role of penetration testers before the simulation. Interestingly, students saw the skill of problem solving as being less important after the simulation. While this finding was counter-intuitive, we speculate that it may be a result of students recognizing the importance of rigidly adhering to ethical principles – something that was strongly emphasized in the storyline – and so may have left them with an impression that cybersecurity professionals do not so much independently solve problems as they apply ethical standards to problems. With some of the other responses are not significant, they are still suggestive. We highlight two here. Students' recognized the importance of communication as part of the requisite skills needed by cybersecurity professionals more after the simulation. Showing a realistic team context, where a strong project manager used authentic communication skills to help facilitate the students' interaction with the simulation, likely played a part in this. Students' confidence in their programming skills also increased after the simulation. We speculate this is due to their work with performing database injections and developing their Linux skills through the simulated Terminal shell.

† p<= 0.10, * p <= 0.05, ** p <= 0.01, *** p <= 0.001.

Our findings are further illustrated in Figs. 7 and 8. Figure 7 shows the differences between the pre and post survey on

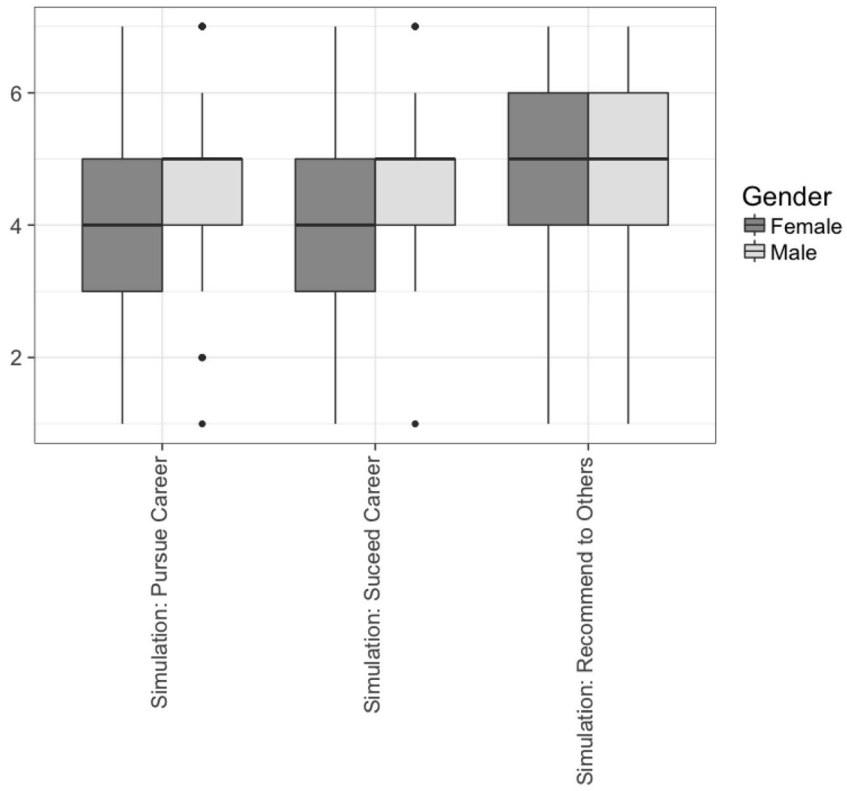

Fig. 6 Boxplots of Postsurvey Questions

Table 2 Statistical Results

Question (difference of 100-point scales)	Pre/Post mean difference (positive is higher postsurvey)	Gender difference of pre/post mean differences (positive is higher female)
Interest in cybersecurity	−1.86 (t=−0.97)	3.83 (t=0.99)
Interest in a cybersecurity career	−0.08 (t=−0.04)	−0.29 (t=−0.06)
Confidence in ability to succeed in career in cybersecurity	2.05 (t=0.88)	10.70† (t=1.98)
Understanding what penetration testers do	**42.50*** (t=12.90)**	9.18 (t=1.30)
Skills: Leadership	3.35 (t=1.50)	4.43 (t=0.90)
Skills: Communication	**3.97* (t=2.28)**	0.15 (t=0.042)
Skills: Adaptability	−2.17 (t=−1.61)	0.31 (t=0.09)
Skills: Problem Solving	**−1.74* (t=−2.06)**	0.60 (t=0.32)
Skills: Ethics	0.23 (t=0.12)	−5.56 (t=−1.24)
Skills: Programming	−1.05 (t=−0.68)	−0.66 (t=−0.22)
Skills: Learn on your own	2.19 (t=1.40)	0.73 (t=0.187)
Skills: Attention to detail	−1.80 (t=−1.57)	−1.85 (t=−0.90)
Confidence: Leadership	1.97 (t=1.22)	5.63† (t=1.83)
Confidence: Communication	1.26 (t=0.83)	**5.59* (t=2.02)**
Confidence: Adaptability	−0.19 (t=−0.12)	1.43 (t=0.36)
Confidence: Problem Solving	0.48 (t=0.38)	−2.15 (t=−0.73)
Confidence: Ethics	**−4.04** (t=−2.63)**	0.13 (t=0.05)
Confidence: Programming	**6.40*** (t=4.13)**	5.45 (t=1.49)
Confidence: Ability to learn	**2.77* (t=2.08)**	2.85 (t=0.76)
Confidence: Attention to detail	−0.86 (t=−0.65)	0.40 (t=0.14)

† $p <= 0.10$, * $p <= 0.05$, ** $p <= 0.01$, *** $p <= 0.001$

what skills students thought that a penetration tester needs to perform their work. Figure 8 shows the differences between the pre and post survey in students' confidence that they could successfully apply those skills.

Qualitative Results Related to Perceptions of Cybersecurity

Responses to the two qualitative questions in the post-survey were analyzed using a thematic analysis process wherein we iteratively identified key themes and patterns in the data. We report these to supplement our quantitative findings above.

When asked how the simulation changed their perceptions of cybersecurity, seven students said that cybersecurity was more complex than they thought. Six students said that cybersecurity was easier than they thought. This is likely due to the different initial perceptions of the field that students held when they experienced Cybermatics. Twenty students said that they became more knowledgeable about cybersecurity after using the simulation. Nine students said they were more interested, while two said they were dissuaded because of the PCS.

When asked why they were not interested in cybersecurity, a variety of reasons were given (Table 3). For instance, eighteen students dislike programming, six said they were not skilled enough, four reported it would be too stressful, while one said it would be too risky. Students also said they did not have enough patience, cybersecurity was too complex, too time consuming, or wanted more human interaction. The differences do not appear to be gender specific.

Qualitative Results about TINAG and Educational Scaffolding

Students also shared many insights about the design elements that they liked and disliked about Cybermatics. Some related to specific implementation details that are not generally useful to designers of other educational simulations. However, a large number of comments related to an important design tension that is inherent in the design of PCSs and related educational simulations. The tension has to do with reconciling the authenticity of the simulation (in the case of Cybermatics the authenticity provided by our TINAG philosophy) with the need to scaffold educational experiences to support students' current capabilities.

As noted, realism was an important attribute of the PCS that students recognized (being specifically mentioned in a positive way by 56% of students). Some comments seem specifically to point towards the value of TINAG, such as a student who noted, "I enjoyed how it allowed you to actually hack and figure things out and how realistic the people felt." Other students described specific components of the PCS that they perceived to be especially realistic, such as one who said, "I really liked how you got to feel like you were really getting into a website and sever. I thought it was cool to be able to perform a real SQL injection." The terminal was especially recognized by students as a helpful component, with 89% of students stating it helped the PCS feel more realistic. One student summarized the value of the terminal by saying:

> I didn't expect it to feel realistic, and it really did. Everything felt well-polished and real, but what really brought the whole simulation together was the Linux terminal. Being able to navigate a workspace like that in a simulated terminal blew me away.

Providing a realistic environment, however, made it difficult to fully support some students in achieving the learning goals of the PCS. 69% of students described needing clearer instructions, better directions, or more help at key moments in the PCS. While all of these are reasonable expectations of a classroom learning experience, each of them can impact TINAG because what is notable about professional

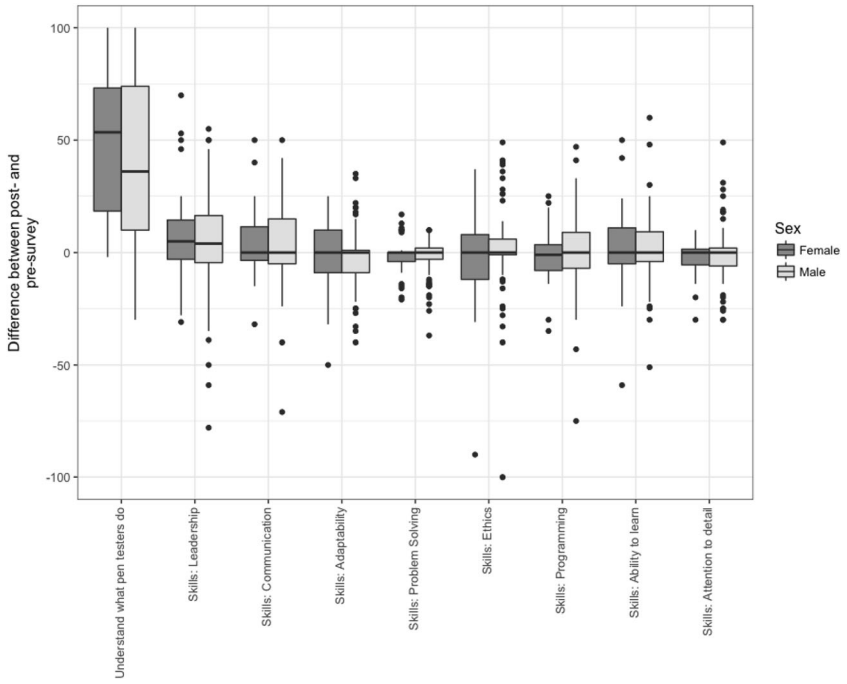

Fig. 7 Understanding Skills Pre- and Post (Segmented by Gender)

environments is often how ambiguous instructions, directions, and other guidelines actually are. Yet as we analyzed comments from the post-survey we recognized that not providing students more background could lead them to become frustrated, overwhelmed, and feel like they did not have the skills needed to complete the tasks. One student said that it would be helpful to have, "better explanation in the documents on how to do what we are supposed to do. For someone who hasn't had very much background it was a little difficult to do in some areas." This type of comment became more pointed from students with little background in technology, such as one who confessed:

> I would not have been able to complete the simulation without the help of the TAs or friends around me. [This class] has been my only experience with coding, security, and computers.. .. I studied the scope document and Googled it but still had trouble figuring out what I

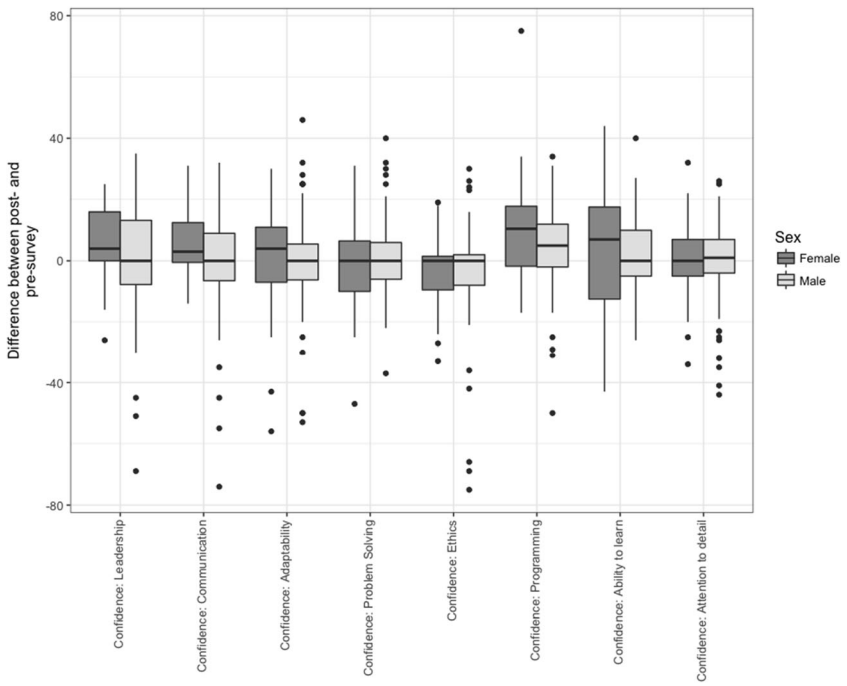

Fig. 8 Confidence Levels of Skills Pre and Post (Segmented by Gender)

Table 3 Reasons Why Students Reported Disinterest in Cybersecurity (Segmented by Gender)

Grouping	Reason	Female	Male
Skills	Linux is hard	1	0
	Programming	7	11
	Confusing parts (security keys, hashcracks)	2	0
	Skill alignment, lack of	3	1
	Not easy to think outside the box / not smart enough	1	1
	Too detail oriented	0	2
	Not enough problem solving	0	1
	Writing	0	1
	Technology	0	1
	Already behind in knowledge	0	2
	Keeping up on new knowledge	0	2
	Too little people skills	0	1
	Too difficult	1	2
	Not enough patience	1	1
	Too time consuming	1	0
Other interests	Topic not interesting	8	6
	I enjoy spending time with kids	1	0
	Prefer other study (art, data science, law, engineering, program management, info science)	6	7
	Into creating	2	1
	Fixing computers rather than hacking	1	0
Profession-related	Not a complete understanding	1	1
	Scary profession	1	0
	Stressful	1	3
	Frustrating	1	2
	Lots of responsibility	0	1
	IT pays more	0	1
	Don't want to be stuck in a cubicle	0	1
	Risks of making a mistake are high	1	1
Miscellaneous	Undecided	1	0
	Work on my own projects	1	0

> needed to do. I got stuck a few times, probably because I am not very good with technology and not completely familiar with IT terms and what the task was asking.

This comment indicates that self-efficacy is tied to the level of educational scaffolding.

Comments about what students did not like about the PCS also highlight this design tension. Some students expressed frustration that there was not always a clear "right answer" to the activities in which they were engaging. For example, a student reported that something to make the simulation better was, "a clear understanding of when a task is finished." While we cannot state for certain what task(s) this student was referring to, we do observe that some tasks in the PCS are intentionally vague, mirroring the vagueness that sometimes accompanies professional practice in the cybersecurity field. Thus, making the PCS more in line with TINAG and authentic practice, was not in line with some students' expectations about educational assignments. Classroom observations also revealed that, while some students seemed to really get into the storyline and participate as if it were real, other students took shortcuts to skip what they considered non-essential narrative in order to quickly finish the assignment. Thus, while providing a clear, unambiguous assignment may meet existing expectations and be less frustrating to students, it is contrary to the goal of providing an authentic experience.

Interestingly, many student frustrations related to moments in the PCS when TINAG was broken. 15% of students reported being bothered when they encountered something in the PCS that broke the expectation for realism that had been built up throughout the experience. While some complaints related to actors who seemed fake, others related to aspects of the PCS that did not allow students to explore beyond the bounds of the programmed scenarios. For example, several students

described how it was bothersome that the SQL injection only responded to certain inputs that the simulation required students to perform. One student aptly stated:

> The Riptech login page seemed to me like a keyword SQL reference. For example, if you put in anything other than exactly what it's looking for, you receive a "query failed" notice. … In essence, I really couldn't explore beyond the immediate scope of the task.

This student, who had prior knowledge about SQL, wanted more realism than the designers were willing to build in, due to their concern that it would be too complicated for those new to the topic.

Discussion

The results presented here suggest that the Cybermatics PCS shows promise as a tool for helping students explore a potential career in cybersecurity at an early stage in their undergraduate education. While only some of our findings rose to the level of statistical significance, we were encouraged by those results that were significant, and find them insightful regarding what PCS simulations like Cybermatics can accomplish in cybersecurity education. In this discussion we comment on the potential value of our findings, and suggest some directions for future research.

We first note that our statistically significant, quantitative findings included both content knowledge student learned, as well as a measure of their confidence about succeeding in cybersecurity as a field. Specifically, some students report a positive change in their content knowledge related to cybersecurity (what it is that penetration testers actually do), and they also developed more confidence in their ability to apply a skill needed by professionals in the field (programming). These effects—that include cognitive and attitudinal outcomes—align with prior research on the benefits of experiential cybersecurity education (Katsantoniset al., 2017), specifically that it can faciliate achievement in multiple domains simultaneously. This, in turn, mirrors how domain-specific knowledge and skills as well as certain dispositions are important to the work of cybersecurity professionals (indeed, professionals in any field). Our findings contribute towards the body of scholarship helping educators to find meaningful ways of integrating many types of outcomes when teaching students who might be preparing for certain careers—even in formative stages such as when they enroll in introductory courses (as was the case for the students who used Cybermatics).

Our qualitative findings provide some additional insight into what can be accomplished by integrated, experiential approaches to learning. The variety of reasons students reported for why their perceptions about cybersecurity changed was quite diverse, suggesting that their personal definitions of constructs like *interest in a cybersecurity career*, or *confidence in their ability to succeed*, were informed by a number of factors. Instructors attempting to support students in their cybersecurity education may have a difficult time predicting all those influences in advance, and so might have a difficult time addressing students' diversity of perception using traditional instructional formats that present the field from a static perspective. Yet, as previous research has found, experiential learning helps students integrate new knowledge and skills into their existing structures of prior knowledge, attitude, and expectations (Kolb and Kolb 2014; Kolb 1984). The richness of the experiential learning environment allows students to make their own connections and draw their own conclusions, without needing an instructor to explicitly predict the places from which students are beginning. So in addition to the value a PCS like Cybermatics might provide in helping students achieve multiple outcomes from one experience, it can also help cybersecurity educators address the diversity of background students bring to their learning experiences, and help them make more personal connections than instructors could distinctly make on their own.

We also suggest that our findings provide suggestions for future research into cybersecurity education, specifically about integrating experiential learning (such as that provided by a PCS) into more formal curricula (cybersecurity courses and programs). As discussed earlier, much of the existing experiential learning in cybersecurity takes the form of competitions or camps, which typically take place as extracurricular activities (Cheung et al. 2012). Yet, to address the need for more qualified cybersecurity professionals we believe that attention must also be given to what is taught in cybersecurity courses themselves (along with how it is taught). While our piloting of Cybermatics provides some insight (ideas for integrating in-class simluation activities with out-of-class assignments), further research is needed that supports educators in more widespread adoption of these types of approaches. Specific issues for research might include how to prepare instructors so they can comfortably teach using an alternative reality approach (such as found in the PCS), whether there are certain kinds of content knowledge, aspects of student interest in a cybersecurity career, or specific areas of confidence that better lend themselves to an alternative reality approach more than others, or what is the contribution towards student learning, interest, and confedence of certain affordances found in the simulation (such as the focus on the This is Not a Game—TINAG—ethos).

As suggested by our design research methodology, we continue to improve the Cybermatics PCS so it can support students in their learning and in their development of cybersecurity career interest and confidence. Some of the qualitative comments our participants provided suggest some ways to

approach future redesigns that will hopefully provide a stronger experience overall, and facilitate changes in students' interest and/or confidence as measured by other of our survey questions, that did not result in statistically significant responses in this research. One of the key findings of our qualitative assessment was the tension between providing an authentic experience (consistent with TINAG), while also providing sufficient educational scaffolding and a necessarily simplified learning experience. TINAG is partially meant to draw students into the simulation and keep interest and engagement high, especially for those bringing some background knowledge to the simulation. But given our goal of increasing student self-efficacy about the topic we cannot ignore students like the one who reported not being "very good with technology." If a PCS is meant to increase self-efficacy, but instead reinforces students' prior mindsets about technology, cybersecurity, or their own abilities to be successful, then the balance between TINAG and denaturing has not been properly achieved. As we review our table of findings (Table 2), we speculate that this may have been the case for some of the areas measured by our survey, even though most of those negative changes were not statistically significant.

Designers of educational products should be careful, then, to provide an appropriate level of scaffolding to facilitate student learning from the model of the environment being taught, recognizing that scaffolding should be commensurate with students' prior experience and should not negatively impact the authenticity of the experience. "Models are necessarily denatured from the real by the medium in which they are expressed. Designers must select a level of denaturing matching the target learner's existing knowledge and goals" (Gibbons 2001, p. 514). This is a balance in the development of PCS simulations that we are still attempting to find. Some of our plans include: (a) refining activities so they are not as difficult for the target audience, while also providing "Easter eggs" for more advanced students to find (and so as to not turn them away from the more basic nature of the standard narrative); (b) providing better educational scaffolding in the form of in-game documents (e.g. documentation), as well as teacher-provided materials and discussions; (c) adding character helps that can be triggered by players (e.g. chat responses to common requests for assistance), and (d) making sure the PCSs are presented to students with the proper background knowledge.

Conclusion

This paper has introduced an example of a new kind of educational simulation, the playable case study (PCS), focused on providing students with a cybersecurity experience embedded in a realistic professional context. It incorporates elements of educational simulations (e.g., virtual internships), case studies, and design principles from ARGs (e.g., TINAG) to create a simplified, yet authentic simulated cybersecurity experience. The data from 111 students from two different U.S. universities who interacted with the Cybermatics PCS helped show the promise of this intervention. Cybermatics increased student understanding about penetration testing, improved their confidence in programming, and increased about half of the students' interest in pursuing a cybersecurity career. Students also reported a number of reasons why their perceptions changed in these areas (both positive and negative). Future research can use these findings to help explore further ways that experiential instruction (like the PCS), that teach content knowledge while also supporting positive changes in student interest and confidence, can be integrated into formal cybersecurity curricula. Our findings also provided insights into a critical design tension between creating authentic experiences (consistent with TINAG) that are also sufficiently scaffolded for newcomers. This can also be a useful finding to designers of educational simulations as they attempt to provide appropriate scaffolds while also providing students with an authentic learning experience. Given the potential value of these findings to other designers, we hope our report of the Cybermatics PCS will lead to additional innovative educational experiences that can help recruit more cybersecurity professionals at this critical time.

Acknowledgment Portions of this paper were previously presented at the 52nd Hawaii International Conference on System Sciences, and are available in the proceedings of that conference.

Funding Funding for part of this work was provided by NSF grant AISL #1323787.

Compliance with Ethical Standards

Declarations of Interest The authors were employed by the universities under study at the time the research took place.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5–14.

Baker, M. (2016). *Striving for effective cyber workforce development*. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_473577.pdf. Accessed 22 Jan 2021.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and

interests predict effectiveness of competitions as a recruitment tool. *Computers & Security, 65*, 153–165. https://doi.org/10.1016/j.cose.2016.10.007.

Battles, J., Glenn, V., & Shedd, L. (2011). Rethinking the library game: Creating an alternate reality with social media. *Journal of Web Librarianship, 5*(2), 114–131.

Bonsignore, E., Hansen, D., Kraus, K., Visconti, A., Ahn, J., & Druin, A. (2013, June). Playing for real: designing alternate reality games for teenagers in learning contexts. In *Proceedings of the 12th International Conference on Interaction Design and Children* (pp. 237–246). New York, NY: ACM.

Bustos, R. A. (2017). Facilitating support of cyber: Toward a new liaison model with cybersecurity education at Augusta. *Journal of Business & Finance Librarianship, 22*(1), 23–31. https://doi.org/10.1080/08963568.2016.1258935.

Center for Cyber Safety Education, (ISC)2, Booz Allen Hamilton, Alta Associates, & Frost & Sullivan. (2017). 2017 *Global information security workforce study benchmarking workforce capacity and response to cyber risk*. Retrieved from https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx. Accessed 22 Jan 2021.

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), 1–8. https://doi.org/10.1115/1.4029235.

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)* (p. 1).

Cornel, C., Cornel, C. M., Rowe, D. C., & Moses, S. (2016, June). A cybersecurity camp for girls. *In Conference for the American Society for Engineering Education*.Washington, DC: ASEE.

Cornel, C. J., Rowe, D. C., & Cornel, C. M. (2017). Starships and cybersecurity: Teaching security concepts through immersive gaming experiences. *Proceedings of the 18th Annual Conference on Information Technology Education - SIGITE, 17*, 27–32. https://doi.org/10.1145/3125659.3125696.

Flushman, T., Gondree, M., Peterson, Z. N. (2015, August). This is not a game: Early observations on using alternate reality games for teaching security concepts to first-year undergraduates. In *8th Workshop on Cyber Security Experimentation and Test ({CSET} 15)*. Berkley, CA: USENIX.

Gavas, E., & Memon, N. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy, 10*(4), 75–79.

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015, November). CyberAware: A mobile game-based app for cybersecurity education and awareness. In *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)* (pp. 54–58). New York, NY: IEEE.

Gibbons, A. S. (2001). Model-centered instruction. *Journal of Structural Learning and Intelligent Systems, 14*, 511–540.

Giboney, J., Hansen, D. L., Johnson, T., Winters, D., McDonald, J. K., Balzotti, J., & Bonsignore, E. (2019, January). Theory of experiential career exploration technology (TECET): Increasing cybersecurity career interest through playable case studies. *52nd Hawaii International Conference on System Sciences*. Wailea, HI: HICSS.

Graham, M. J., Frederick, J., Byars-Winston, A., Hunter, A.-B., & Handelsman, J. (2013). Increasing persistence of college students in STEM. *Science, 341*(6153), 1455–1456.

Gredler, M. E. (2004). Games and simulations and their relationship to learning. In D. H. Jonassen (Ed.), *Handbook of research on educational communications and technology* (2nd ed., pp. 571–582). Mahwah, NJ: Lawrence Erlbaum Associates Inc.

Hansen, D. L., Balzotti, J., Fine, L., & Ebeling, D. (2017, January). Microcore: A playable case study for improving adolescents' argumentative writing in a workplace context. *50th Hawaii International Conference on System Sciences*. Waikoloa Village, HI: HICSS.

Heitzmann, R. (2008). Case study instruction in teacher education: Opportunity to develop students' critical thinking, school smarts and decision making. *Education, 128*(4), 523–542.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

Holm, S. (1979). A simple sequentially rejective multiple test procedure. *Scandinavian Journal of Statistics, 6*(2), 65–70.

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.

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. https://doi.org/10.1177/0735633116651971.

Johnston, J. D., Massey, A. P., & Marker-Hoffman, R. L. (2012). Using an alternate reality game to increase physical activity and decrease obesity risk of college students. *Journal of Diabetes Science and Technology, 6*(4), 828–838.

Katsantonis, M., Fouliras, P., Mavridis, I., & (2017, April). Conceptual analysis of cyber security education based on live competitions. In,. (2017). *IEEE Global Engineering Education Conference (EDUCON)* (pp. 771–779). New York, NY: IEEE.

Kay, D. J., Pudas, T. J., & Young, B. (2012). Preparing the pipeline: The U.S. cyber workforce for the future. *Defense Horizons, 72*(August), 1–16.

Kolb, A. Y., & Kolb, D. A. (2014). Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of Management Learning & Education, 4*(2), 193–212.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and developmen*. New Jersey: Prentice-Hall.

LeClair, J., & Pheils, D. (2016). Women in cybersecurity. Albany: NY: Excelsior College.

McDonald, J. K., Hansen, D. L., Balzotti, J., Tanner, J., Winters, D., Giboney, J., & Bonsignore, E. (2019, January). Designing authentic cybersecurity learning experiences: Lessons from the Cybermatics playable case study. *Proceedings of the 52nd Hawaii International Conference on System Sciences, 6*, 2507–2516. Wailea, HI: HICSS.

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K., & Impagliazzo, J. (2014, March). Toward curricular guidelines for cybersecurity. In *Proceedings of the 45th ACM technical symposium on Computer science education* (pp. 81–82). New York, NY: SIGCSE.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)* (pp. 256–262). New York, NY: IEEE.

Niemeyer, G., Garcia, A., & Naima, R. (2009, October). Black cloud: patterns towards da future. In *Proceedings of the 17th ACM International Conference on Multimedia* (pp. 1073–1082). New York, NY: ACM.

Nunamaker Jr., J. F., & Briggs, R. O. (2011). Toward a broader vision for information systems. *Transactions on Management Information Systems, 2*(4) 20, 1–20. https://doi.org/10.1145/2070710.2070711.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77.

Pellicone, A., Bonsignore, E., Kaczmarek, K., Kraus, K., Ahn, J., & Hansen, D. (2017). Alternate reality games for learning: A frame by frame analysis. *Alternate Realities Games and the Cusp of Digital Gameplay, 5,* 78.

Raj, R. K., & Parrish, A. (2018). Towards standards in undergraduate cybersecurity education in 2018. *Computer, 51*(2), 72–75. https://doi.org/10.1109/MC.2018.1451658.

Raytheon (2016). *Securing our future: Closing the cybersecurity talent gap*. Sterling, VA: Raytheon Company. Retrieved from https://www.raytheon.com/sites/default/files/cyber/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf. Accessed 22 Jan 2021.

Rowland, P., Podhradsky, A., & Plucker, S. (2018, January). CybHER: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *In Proceedings of the 51st Hawaii International Conference on System Sciences* (pp. 3727–3735). Waikoloa Village, HI: HICSS.

Schank, R. C. (1994). Goal-based scenarios: A radical look at education. *The Journal of the Learning Sciences, 3*(4), 429–453.

Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care?: Exploring the implications of the 2014 NIST Cybersecurity framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal, 50*(2), 303–354.

Shaffer, D. W. (2004). Pedagogical praxis: The professions as models for postindustrial education. *Teachers College Record, 106*(7), 1401–1421.

Shaffer, D. W. (2005). Epistemic games. *Innovate: Journal of Online Education, 1*(6), 2.

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* (pp. 1–14). New York, NY: ACM.

Tims, H. E., Turner, G. E., Corbett, K., Deemer, E. D., & Mhire, J. (2014). Cyber value and interest development: Assessment of a STEM career intervention for high school students. *Electronic Journal of Science Education, 18*(1), 1–15.

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.

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal, 4*(2), 32–46.

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in cyber security education: The MIT Lincoln Laboratory capture-the-flag exercise. In *Proceedings of the 4th conference on Cyber Security Experimentation and Test* (p. 12). New York, NY: ACM.

Yang, S. C., & Wen, B. (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States. *Journal of Education for Business, 92*(1), 1–8. https://doi.org/10.1080/08832323.2016.1261790.