International Journal of STEM Education for Sustainability, Vol.3, No.1, 2023, pp. 47-67
e-ISSN 2798-5091. DOI. 10.52889/ijses.v3i1.132

Addressing Cybersecurity Challenges in Education

Submitted 29 June 2022, Revised 20 August 2022, Accepted 20 August 2022

William J. Triplett[1]

[1]Cybersecurity Leadership Program, Capitol Technology University, Laurel, United States
Coresponding Email: *wjtriplett@captechu.edu:

Abstract

This study aimed to address the challenges of cybersecurity in education. As kindergarten through twelfth-grade education shifts to online and remote learning, educators and governments are increasingly vulnerable to the risks of cyberattacks and cybercrimes. This study focused on the strategies that institutions can employ to increase their students' cybersecurity awareness and simultaneously motivate them to pursue cybersecurity as a career. To achieve the research objectives, a systematic review of ten studies was performed, and the results showed that game-based strategies were effective in increasing students' awareness about cybersecurity and their interest in pursuing cybersecurity as a career. The study's implications suggest that game designers and developers may want to develop advanced games that gauge students' cybersecurity skills and ability to respond to aggressive forms of cyberattacks in addition to enhancing their knowledge of cybersecurity.

Keywords: Cybersecurity, Game-based strategies, K–12 education

INTRODUCTION

As the world strives to protect and uphold the privacy of data and information shared through different computer systems, there are concerns about whether primary and secondary education, together with government training programs, can train individuals who can mitigate the increased risks of cyberattacks and cybercrimes in K–12 online education (Domeij, 2019). The adoption of technology in learning institutions has not only improved the delivery of remote learning but has also increased the severity of cybersecurity risks experienced by schools and individual students (Hasib, 2018). Currently, cybersecurity leadership and the federal government face extensive challenges in K–12 learning, particularly given the major shifts due to the coronavirus 2019 (COVID-19) pandemic. Failure to standardize cybersecurity professionalization and resolve talent scarcity is perpetuating the existing shortfalls and struggles (Wright, 2016). Amid global uncertainty linked to the physical closure of schools, implementation of remote learning and work schedules for students and federal agencies, and the challenges associated with COVID-19, cybersecurity challenges have only increased. Therefore, the failure to standardize the cybersecurity professionalization and resolve talent scarcity in cybersecurity will only worsen the existing cybersecurity challenges in schools and government agencies (Wright, 2016).

Cybersecurity is a crucial and rapidly growing area in information technology (Dunn & Merkle, 2018). However, despite the growth, researchers have raised concerns about the availability of cybersecurity specialists (Dunn & Merkle, 2018; Filipczuk et al., 2019; Hart et al., 2020; Mountrouidou et al., 2019). Mountrouidou et al. (2019) asserted that the rate of cyberattacks and cybercrimes have increased the demand for cybersecurity professionals. In particular, Mountrouidou et al. (2019) cited a global survey that reported that in the United States, there were at least 59% vacancies for cybersecurity analysts. Companies with such vacancies also announced an 82% risk of being cyberattacked (Mountrouidou et al., 2019). Similar findings were reported by Hart et al. (2020), who found a significant association between the rates and sophistication of cyberattacks and the number of cybersecurity specialists available to mitigate such attacks. Overall, the scarcity of cybersecurity specialists increases the vulnerability of individuals, companies, and institutions of learning to hackers.

Researchers worldwide have echoed the concern raised by Mountrouidou et al. (2019) that there is a significant shortage of cybersecurity professionals and specialists. For instance, while Mountrouidou et al. (2019) found that 2,300 heads of companies reported a 59% shortage of cybersecurity staff, Choudhury (2022) reported that the sustained cyberattacks and increased cybercrimes globally could be attributed to the shortage of cybersecurity professionals. In a previous study conducted by Nobles (2018), it was established that as of 2017, the global cybersecurity talent gap was two million. That is, as of 2017, the world suffered a shortage of 2 million cybersecurity professionals. In their findings, Choudhury (2022) reported that the world was lacking more than 3 million cyber professionals who could provide cyber leadership and train, test, and secure digital systems used by people. Although Drmola et al. (2021) and Angafor et al. (2020) failed to give the actual figures regarding the shortage of cybersecurity professionals, they concurred with other researchers that the world was facing a massive shortage in computer and cybersecurity specialists.

As Choudhury (2022) discussed, the shortage of cybersecurity officials has left businesses, learning institutions, and government agencies exposed to cyberattacks. A shortage of 3 million cybersecurity specialists means the world is missing out on advanced cybersecurity systems that can test and secure technological systems from being manipulated and controlled by hackers. Some researchers have also discussed the reasons for the significant shortage of cybersecurity specialists. In one such study, Armstrong et al. (2018) reported that the lack of qualified professionals to guide high school and college students on pursuing cybersecurity as a career is a significant contributor to the shortage. They found qualified cybersecurity professionals to act as mentors and advisors to the younger generation of children interested in cybersecurity. However, the scarcity of cybersecurity specialists limited the number of mentors students can emulate and seek guidance from.

The lack of mentors has limited the number of women willing to become cybersecurity specialists. Hodhod et al. (2019) found that the cybersecurity talent gap was partly driven by the lack of women taking up the challenge of pursuing a career in cybersecurity. The lack of experts to guide and mentor young girls into becoming cybersecurity specialists discouraged many, thus sustaining the talent shortage. Pinchot et al. (2020) supported the findings of Hodhod et al. (2019) in a qualitative research with 25 students that found that the lack of peer mentors demotivated women and increased their chances of leaving information technology and security courses. Similarly, Burrell (2020) reported that a lack of experts and professionals in cybersecurity discouraged young minds from pursuing a career in cybersecurity as there are no role models or mentors to guide them. Overall, the scarcity of cybersecurity specialists has not only discouraged students, especially girls, from becoming cyber-specialists but has also deprived schools of a content-driven cybersecurity curriculum.

Researchers have argued that the scarcity of cybersecurity specialists is partly fueled by a shortage of cybersecurity programs in high schools and colleges. For instance, Smith (2018) posited that the limited number of specialists and the skill shortage in cybersecurity limited the knowledge pool that could develop a robust cybersecurity curriculum for high school and college students. Armstrong et al. (2018) reiterated that the cybersecurity courses and training offered to students were of low quality and did not match the skills required by employers in the cybersecurity sector. The employment rejection suffered by cybersecurity graduates discouraged others from enrolling in cybersecurity courses and programs. Sanzo et al. (2021) reiterated that while schools have tried to update their information security courses, the scarcity of specialists has made it virtually impossible for schools to maintain pace with the changing cybersecurity environment. Alrabaee et al. (2022) concurred with Sanzo et al. (2021) that the lack of standardized cybersecurity educational programs and challenges experienced when updating the courses and the notion that cybersecurity graduates are ill-equipped with the skills needed for the job market discouraged students from pursuing cybersecurity as a career.

The lack of mitigation strategies and resources, including cybersecurity professionals and computer specialists, allows hackers to steal sensitive individual, company, and student information from institution servers. Filipczuk et al. (2019) presented evidence of the increased risks of cyberattacks due to the scarcity of cybersecurity specialists. They found that hackers took advantage of the few specialists available in the education sector to target school and student information. Similar conclusions were reported by Oyedotun (2020), who found that the shift to remote learning increased students' susceptibility to phishing and social engineering attacks. Many learning institutions at the time of the COVID-19 outbreak lacked computer specialists to offer teachers and students practical training on technology and the risks of cyberattacks. As the education sector grappled with the challenges of COVID-19, Khan et al. (2020) identified the cybersecurity threats that institutions and students experienced during online learning: DDoS attacks and malicious domains, mobile learning apps, websites, and social media messages. Jayakumar et al. (2020) suggested the need for cybersecurity awareness and training for both students and instructors to mitigate the negative impacts of such cyberattacks.

Education plays a crucial role in enhancing cybersecurity awareness. K–12 instruction occupies an important position in tackling this deficiency by increasing understanding of the relevance of cybersecurity and allowing learners to acquire essential expertise to engage in cybersecurity career paths (Javidi & Sheybani, 2018). Technological and cybersecurity awareness has become an important skill in the job market and has increased the need for early student training on cybersecurity to address the current shortage of cybersecurity professionals (Garba et al., 2020). The academic world has been a target of various cyber incidents. However, only a few schools possess the resources to effectively counter security incidents and create awareness about cybersecurity incidents among their students and instructors (Coleman & Reeder, 2018). The inadequacies of resources and increased risks of cyberattacks against schools have raised concerns about the cybersecurity status of K–12 schools.

Other challenges include insufficient funding and failing to offer learners valuable cybersecurity schooling. In numerous institutions, cybersecurity classes are elective courses. Most learners complete their K–12 education without having taken a specific cybersecurity course. Cybersecurity is frequently consolidated with electives but should be a universal foundational subject. The task, currently, is for universities to reconsider methods of training students in cybersecurity. Correspondingly, corporate advisors should provide cybersecurity instruction to increase the number of experts joining the industry. The absence of cybersecurity proficiency and the expanding disparity between demand and resources calls for urgent measures to be taken at the institution level (Fourie et al., 2014).

Addressing the Scarcity of Cybersecurity Professionals

The scarcity of cybersecurity specialists has increased the risks of cyberattacks, resulted in poor-quality cybersecurity programs, and discouraged high school and college students from pursuing a career in cybersecurity. To address the negative outcomes of cybersecurity specialists, researchers have investigated and reported on some strategies used to attract and motivate students to select cybersecurity as a career. One of the strategies that researchers have championed is increasing cybersecurity awareness among high school and college students. With the outbreak of COVID-19 and the suspension of in-person learning, instructors have found an opportunity to increase students’ awareness regarding cybersecurity as a career choice. The risks of being hacked or receiving suspicious emails and website links have increased remote students' vulnerability to hackers who steal their private information (Sanzo et al., 2021). Caspary and Warner (2016) reported that vocation-themed pathways incorporating introductory cybersecurity instruction, specialized training, and practical application of cybersecurity skills motivated students to specialize in cybersecurity.

The role of cybersecurity awareness in increasing the number of students willing to specialize in cybersecurity has also been supported by government agencies. For instance, the National Initiative for Cybersecurity Education, directed by the National Institute of Standards and Technology in the Department of Commerce, has collaborated with high schools and colleges to design courses and programs that will attract students and provide them the training that befits a cybersecurity specialist (Wright, 2016). The DHS has partnered with K–12 schools to supply information technology teachers with the necessary academic materials and training to train their students and increase cybersecurity awareness (Alrabaee et al., 2022). The programs designed by the collaboration of government agencies incorporate complex cybersecurity scenarios, practical cyberattack training, and the skills to counter such attacks. Hart et al. (2020) found that real-life training of students on cybersecurity increased their curiosity about cyberattacks and the software used to mitigate such attacks. The curiosity developed through cybersecurity awareness motivated students to pursue a career in cybersecurity.

The shortage of qualified cybersecurity professionals requires that institutions of learning work to retain their cybersecurity specialists and also design programs that can be implemented to increase the number of students willing to become cybersecurity professionals and leaders in the future (Finch et al., 2020). Introducing cybersecurity courses and concepts into K–12 curricula effectively increases the number of students willing to choose a career in cybersecurity (Finch et al., 2020; Nobles, 2018). Recommended elective courses for preparing cybersecurity professionals at the high school level are not limited to Introduction to Cybersecurity, Digital Forensic Investigation Techniques, Intrusion Analysis and Response, and Introduction to Human Factors in Cybersecurity (Finch et al., 2020). Given the difficulty of implementing major changes to the public-school curriculum, charter schools, with their greater autonomy, may be more amenable forums for developing these course offerings (Finch et al., 2020).

Educators have discovered that students in high school and college have become increasingly interested in studying cybersecurity; thus, in addition to introductory courses, they have designed seminars to expand the students' knowledge of cybersecurity. For instance, Moallem (2019) quantitatively investigated cybersecurity awareness among college students and found that many were unaware of methods of data protection from hackers. However, engaging these college students in cybersecurity awareness seminars enhanced their knowledge and even motivated them to become cybersecurity professionals. Similar results were reported by Smith and Ali (2019), who found that encouraging students to participate in GenCyber summer camps and National Cyber Security Awareness Month improved their knowledge of cyber threats and likely means of attacks. In an earlier study, Jin et al. (2018) also found that students who participated in GenCyber summer camps developed cybersecurity awareness and interest in becoming cybersecurity professionals. Thus, researchers have established that, similar to educational courses, seminars enhance students' cybersecurity awareness and motivate them to choose a career in cybersecurity.

Corporations have also signed cooperation agreements with learning institutions to increase the number of students training to become cybersecurity professionals. Srivatanakul and Annansingh (2021) found that corporations helped institutions of learning to design cybersecurity courses and training programs based on the requirements and skillset that cybersecurity specialists should possess. The collaboration between colleges and organizations has ensured that students undertaking cybersecurity courses can access practical training from such organizations through internships. The availability of internship opportunities in corporate organizations that expose students to real-life cybersecurity challenges and the risks associated with important information in the hands of hackers increases students' motivation to become professionals in cybersecurity. Besides internship and apprentice opportunities, increasing the salaries earned by cybersecurity professionals is another motivation to increase the number of students training to become cybersecurity professionals (Bordel et al., 2022). Overall, increasing student awareness about the importance of cybersecurity professionals in protecting data and securing systems, providing them with the relevant and most current training and resources, and increasing their salaries will increase the number of students willing to make a career in cybersecurity.

METHOD

A systematic review of studies was conducted to investigate the strategies that institutions of learning can employ to increase their students' cybersecurity awareness and simultaneously motivate them to pursue cybersecurity as a career (Pati & Lorusso, 2018). The review found that there is a significant gap in the literature and in practice regarding the availability of computer and cybersecurity specialists who can mitigate the increased cases of cyberattacks (Dunn & Merkle, 2018; Filipczuk et al., 2019; Hart et al., 2020; Mountrouidou et al., 2019). As Hart et al. (2020) found, the outbreak of COVID-19 and the requirement that employees work remotely and students be engaged in remote learning increased the vulnerability of such individuals to targeted cyberattacks. The COVID-19 pandemic also evidenced the significant shortage of cybersecurity specialists in learning institutions, thereby leading to the inability of these institutions to mitigate their vulnerability to cyberattacks. Therefore, this study aimed to investigate the use of digital games to increase student awareness of cybersecurity and increase their interest in cybersecurity as a career to address the scarcity of cybersecurity specialists.

To justify the existence of a problem and gap in the literature, the researcher followed the systematic review protocol to search for information. For instance, Pati and Lorusso (2018) stated that researchers conducting systematic reviews of literature must adhere to the following guidelines: systematic searching of relevant literature, filtering of the identified literature, reviewing the selected studies, critiquing the literature, interpreting the literature, and reporting the findings from different perspectives of reviewed studies. Therefore, in the search for relevant literature, the researcher developed a set of inclusion and exclusion criteria to maximize and improve the quality of the studies selected. For inclusion, the study must be a) a peer-reviewed journal article, b) published in English, c) published within the last 5 years, d) must have participants who are high school and university students, and e) must be about digital games used to increase cybersecurity awareness.

The researcher excluded studies that were not peer-reviewed, not published in English, did not include high school and university students, and were not published within the last 5 years. The inclusion and exclusion criteria used in systematic review studies are intended to guide the reader on the types and characteristics of the studies included in the systematic review (Ahn & Kang, 2018). The set criteria also guide and save the researcher from individually analyzing published studies that might be time-consuming (Ahn & Kang, 2018). To ease the search and selection of relevant published studies, the researcher developed a set of keywords and search terms. The search terms included *cybersecurity, strategies to increase cybersecurity awareness*, *game-based approach to cybersecurity awareness*, *gamification of cybersecurity*, *and cybersecurity career awareness*.

The above search terms were keyed in the following educational bases: Google Scholar, ScienceDirect, ERIC, IEEE Xplore, Sage, Wiley, and MDPI. To ensure that the articles met the inclusion criteria, the researcher read the abstracts of the published materials; based on the abstracts, the decision on whether to include or exclude the study was made. The initial review of the literature yielded a huge volume of research on the strategies used to address the scarcity of cybersecurity specialists and increase students' cybersecurity awareness. However, most studies were found to be irrelevant, although published in English and within the last 5 years. After filtering and analysis, the researcher systematically reviewed a total of ten qualitative, quantitative, and systematic review studies on the cybersecurity leadership challenges in education. Table 1 shows the articles that were reviewed, their purposes, methodologies, number of participants, findings, and suggestions.

Table 1. Articles Reviewed on Cybersecurity Leadership Challenges in Education

Citations	Purpose	Methods	Participants	Findings	Suggestions
(Filipczuk et al., 2019)	To explore the effectiveness of digital games in enhancing employee	Qualitative descriptive research to explore the effectiveness of	17 participants	15 of the 17 participants reported increased awareness of	Extensive research to explore employees' opinions

Citations	Purpose	Methods	Participants	Findings	Suggestions
	cybersecurity responsibility	m-learning games in increasing cybersecurity awareness among employees		cybersecurity issues such as phishing attacks, social engineering attacks, benefits of data protection, and types of malware attacks. The mobile-based gaming was found to be flexible, fun, and quick to learn	regarding their organizations' role in combating cyber threats. Future researchers should seek to definitively measure the outcomes of high-order learning through cyber literacy games using bloom taxonomy
(Jin et al., 2018)	To investigate the effectiveness of GenCyber high school summer camp using game-based learning to increase cybersecurity education and as a career for students	Quantitative research method with post-camp survey questions	200 students from the Chicago Metropolitan areas	Four different games were designed: social engineering games, a secure online behavior game, a Cyber defense tower game, and a 2D GenCyber card game. The games exposed students to cybersecurity principles and secure online behaviors. Instructors and support staff	More research on games that will appeal more to women as the current games were found to be more fun and effective for male students compared to female students

Citations	Purpose	Methods	Participants	Findings	Suggestions
				found the games to be effective in guiding the students' educational interest and professionalism in cybersecurity	
(Mountrouidou et al., 2019)	To investigate the effectiveness of game-based strategies in attracting students to study cybersecurity and increase the population of cybersecurity specialists	Systematic review of literature: open literature and focused literature search	82 studies were selected and analyzed	Introductory courses on cybersecurity and summer camps such as GenCyber gamification were found to not only increase cybersecurity awareness but also motivate students to become computer specialists	Future researchers should develop strategies that would increase the population of minority students in cybersecurity courses and specializations. Research should also be conducted to assess the cybersecurity preparedness of universities and areas of improvement
(Yasin et al., 2019)	To design a serious game that increases individual software security awareness	Quantitative research methodology	96 participants	The cybersecurity requirement awareness game was found to increase students' knowledge of	More serious interdisciplinary games should be developed to enhance student engagement with cybersecurity

Citations	Purpose	Methods	Participants	Findings	Suggestions
				cyberattacks and countermeasures, and increased their interest in becoming cybersecurity and computer specialists	and motivate them to develop countermeasures against common cyberattacks
(Hart et al., 2020)	To examine the effectiveness of Riskio, a tabletop game to increase cybersecurity awareness among students and people with limited technical background	Quantitative experimental research methodology	54 participants were included in the study	Riskio created an active learning environment where learners were trained to develop cyberattacks and countermeasures themselves	Future researchers should design and implement serious games compatible with the university curriculum, to motivate students to become computer specialists
(Alqahtani & Kavakli-Thorne, 2020)	To design and evaluate the effectiveness of augmented reality game for cybersecurity awareness	Quantitative experimental research method with pre- and post-application survey	91 participants	The augmented reality game was found to increase students' understanding of cybersecurity attacks, vulnerabilities, and countermeasures	Future researchers seeking to advance CybAR games application in education should consider incorporating risky cybersecurity behaviors to examine the impacts of user efficacy and

Citations	Purpose	Methods	Participants	Findings	Suggestions
					cybersecurity threat avoidance
(Tobarra et al., 2021)	To evaluate the effectiveness of a cloud-based game in enhancing students' interest in cybersecurity professionalism	Quantitative research method		Cyberscratch, a cloud-based game was found effective in motivating and engaging students in practical cybersecurity activities. The game was found to improve students' knowledge on the data privacy, storage, and visualization. The students also reported critical thinking skills and abilities for a career in cybersecurity	Future scholars should consider expanding Cyberscratch engine to enable instructors design their cybersecurity games based on their school's cybersecurity curriculum
(Giboney et al., 2021)	To increase students' cybersecurity awareness and career interest using playable case studies	Quantitative methods research	111 students	PCS Cybermatics was found to increase the students' understanding of the professional aspects of cybersecurity work, improve confidence to apply their	Additional research on innovative educative means of training and engaging students in cybersecurity is still needed

Citations	Purpose	Methods	Participants	Findings	Suggestions
				cybersecurity skills, and increase the number of students interested in making a career out of cybersecurity	
(Stoker et al., 2021)	To investigate the efficiency of game-based strategies in apprenticeship programs to increase students' cybersecurity awareness	Quantitative research method	94 college students	The findings revealed that the CyberStart Go used in the apprenticeship program enhanced students' cybersecurity awareness and allowed students the opportunity to practically apply cybersecurity theory during the apprenticeship	The researchers recommended that schools should partner with organizations with workable apprenticeship programs to expose students to real-world cybersecurity challenges
(Coenraad et al., 2020)	To evaluate the effectiveness of the games used to increase students' awareness of cybersecurity and cyberattacks	Systematic review of literature	181 games from Apple App Store, Google play store, Steam, and general web	Games were found to increase student awareness of cybersecurity and improve students' deep content and practical engagement with	Future game designers should consider shifting from presenting cybersecurity through games to focusing on cyber safety

Citations	Purpose	Methods	Participants	Findings	Suggestions
				computers, which increased their interest in picking a cybersecurity career	

RESULTS AND DISCUSSION

Ten studies were reviewed to examine the efficacy of game-based learning as a strategy used by institutions of learning to increase students' awareness of cybersecurity and encourage the pursuit of cybersecurity as a career. Of the ten studies, one was a qualitative research study that explored the efficacy and the perception of students regarding the role of games in enhancing cybersecurity awareness. Two studies employed systematic reviews of literature examining the use of digital games from the Apple App Store and Google Play Store in creating cybersecurity awareness among students. The remaining seven studies used quantitative experimental research methodologies to examine how effective game-based learning was in increasing students' cybersecurity awareness and their subsequent interest in cybersecurity as a career and profession.

Analysis of the reviewed studies revealed that more research was needed on using games as a strategy not only for attracting and increasing students' awareness of cybersecurity and threats but also for enhancing cyber safety. Overall, the researchers concluded that the practical game-based approach effectively engaged students and equipped them with the skills to identify and counter different cyberattacks. It was also established that allowing students to play characters of both the attacker and defender equipped them with the skills needed to anticipate how they might be attacked and thus take appropriate measures. The challenges faced by children when playing these games were found to stimulate their desire to pursue cybersecurity as a career.

This systematic review aimed to investigate the strategies that can be used by institutions of learning, especially high schools, and colleges, to increase the number of students training to become cybersecurity professionals. The objective of motivating students to become cybersecurity professionals is to address the shortage of people with such important skills.

Mountrouidou et al. (2019) found that while the demand for cybersecurity professionals in the United States is expected to experience a growth rate of up to 28%, security managers report that the number of cybersecurity professionals is not enough to fill the existing 59% of unfilled positions.

Mountrouidou et al. (2019) reported that many organizations anticipated an 82% rate of cyberattacks due to the shortage of trained individuals to secure computers and computer systems. Similar findings were reported by Wolfenden (2019), who found that despite increased digital connections, the United States suffers from a significant cybersecurity skills gap, with more than 300,000 cybersecurity personnel positions opened across the United States. Globally, the number of unfilled cybersecurity vacancies keeps shifting, with the most recent data by Choudhury (2022) indicating that the world is short of 3 million cybersecurity professionals. In 2017, Nobles (2018) determined a worldwide shortage of 2 million cybersecurity professionals. This scarcity of cybersecurity professionals prompted the researcher to investigate the effectiveness of game-based strategies to increase the number of students willing to pursue cybersecurity as a profession.

The review of the ten studies revealed that institutions of learning were keen to develop strategies that students will find fun and engaging, such as game-based strategies. In the systematic review conducted by Mountrouidou et al. (2019), it was evident that students found game-based strategies effective in increasing cybersecurity awareness and interest in cybersecurity as a career. Mountrouidou et al. (2019) found that combining digital games on cybersecurity with summer camps such as GenCyber, allowed students to enjoy learning about cyberthreats, cyberattacks, and mitigation measures. Similar findings were reported by Coenraad et al. (2020), who analyzed 181 cybersecurity games from the Apple App Store and Google Play Store and reported improvement in students’ knowledge of cybersecurity and interest in cybersecurity as a profession. Although Coenraad et al. (2020) did not investigate the role of summer camps such as GenCyber, they reported that students who developed an interest in cybersecurity were drawn into deeper cybersecurity safety content.

Besides the systematically reviewed studies, the qualitative studies included in the systematic review also explored the effectiveness of mobile-based learning games in increasing college student awareness and interest in cybersecurity. Analyzing responses from 17 of the students in the study by Filipczuk et al. (2019), 15 reported that through the m-learning game, they became aware of the different cybersecurity attacks such as phishing and appreciated the role of cybersecurity professionals in preventing such attacks. Similar conclusions were reported in the quantitative experimental studies included in the systematic review. Agreeing with Filipczuk et al. (2019), Jin et al. (2018) found that social engineering games, cyber defense tower games, and 2D GenCyber Card games did not only equip students with cybersecurity knowledge but also allowed them the opportunity to play as cyber-attackers and sometimes defenders. The opportunity to practically learn about cybersecurity and play both scenarios was found to interest students and increase their willingness to become cybersecurity professionals.

Yasin et al. (2019) and Hart et al. (2020) designed and evaluated the effectiveness of serious tabletop games in increasing the number of students willing to pursue cybersecurity as a career and gain cybersecurity knowledge. In the combined sample of 154 college and high school students, Yasin et al. (2019) and Hart et al. (2020) found serious tabletop games and Riskio games to improve students' critical thinking, motivate them to learn about cybersecurity, and increase their interest in the cybersecurity profession. Giboney et al. (2021) studied PCS cybermatics games and supported the findings of Hart et al. (2020) that cybersecurity awareness games increased students' cybersecurity knowledge, skills, and interest in becoming cybersecurity professionals. Stoker et al. (2021) found CyberStart Go to promote college students' interest in cybersecurity specialization as a career as the game provided students the opportunities to practically employ their theoretical cybersecurity skills in real life. The above conclusions were supported by Tobarra et al. (2021) and Alqahtani and Kavakli-Thorne (2020), who found that cloud-based games, such as CyberScratch and augmented reality games, provided college students the opportunity to apply their skills in evading and preventing cyberattacks. Although these experiences were not real-life, the games were found to activate the students' memories and provide simulations that pitched them against cyber threats.

Notably, while there are several strategies that schools can use to train their students on cybersecurity, Jin et al. (2018) reported that such measures did not cover all aspects of cybersecurity. However, the authors found that game-based strategies engaged students in identifying cyber threats, simulating defense mechanisms, and allowing them to design their own games based on their knowledge of cybersecurity. Alqahtani and Kavakli-Thorne (2020) found that games such as CyberScratch allowed instructors to guide students in developing cybersecurity games based on their knowledge and area of interest in the cybersecurity profession. The opportunity allowed students to practice their knowledge and gauge their understanding of cybersecurity threats and the required mitigation measures. Overall, cybersecurity games are designed in ways that stimulate students' interest to learn about cybersecurity and motivate them to become cybersecurity professionals.

CONCLUSION

The analysis of the studies in this systematic review reveals a significant shortage of cybersecurity professionals. The scarcity of cybersecurity professionals negatively affects the population and quality of mentors available to students seeking to become cybersecurity professionals and impacts the quality of training such students receive. Lack of mentorship, poor training, and lacking the necessary cybersecurity skills needed to secure employment in the information security sector has discouraged many students from selecting cybersecurity as a career. This paper aimed to identify strategies to address the cybersecurity challenges in education, such as the scarcity of cybersecurity professionals to teach and train students, while increasing the number of those willing to become cybersecurity professionals. From the systematic review of literature, it was evident that game-based strategies are effective in increasing students' cybersecurity awareness and their decision to become cybersecurity professionals. To solve the scarcity of cybersecurity professionals, the researcher established that increasing the number of students willing to choose cybersecurity as a career and providing them the necessary support until graduation proved effective.

SUGGESTION

The games reported in the peer-reviewed studies focused on increasing students' cybersecurity awareness and did not necessarily examine their skills in cybersecurity. For future research, game designers and developers may want to develop advanced games that gauge the students' cybersecurity skills and ability to respond to aggressive cyberattacks in addition to enhancing their knowledge of cybersecurity.

ACKNOWLEDGMENT

The author received no financial support for the research, authorship, and/or publication of this article.

REFERENCES

Ahn, E. J., & Kang, H. (2018). Introduction to systematic review and meta-analysis. Korean Journal of Anesthesiology, 71(2), 103–112. https://doi.org/10.4097/kjae.2018.71.2.103

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information, 11(2), 121. https://doi.org/10.3390/info11020121

Alrabaee, S., Al-Kfairy, M., & Barka, E. (2022). Efforts and suggestions for improving cybersecurity education. 2022 IEEE Global Engineering Education Conference (EDUCON), 1161-1168. https://doi.org/10.1109/educon52537.2022.9766653

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Bridging the cyber security skills gap: Using tabletop exercises to solve the CSSG crisis. In M. Ma, B. Fletcher, S. Göbel, J. Baalsrud Hauge, & T. Marsh (Eds.), Serious games (pp. 117–131). Springer. https://doi.org/10.1007/978-3-030-61814-8_10

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2018). The knowledge, skills, and abilities used by penetration testers: Results of interviews with cybersecurity professionals in vulnerability assessment and management. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62(1), 709–713. https://doi.org/10.1177/1541931218621161

Bordel, B., Alcarria, R., & Robles, T. (2022). A cybersecurity competition to support the autonomous, collaborative, and personalized learning in computer engineering. 2022 IEEE Global Engineering Education Conference (EDUCON), 1346-1354. https://doi.org/10.1109/educon52537.2022.9766611

Burrell, D. N. (2020). An exploration of the cybersecurity workforce shortage. In Management Association, Information Resources (Eds.), Cyber warfare and terrorism (pp. 1072–1081). IGI Global. https://doi.org/10.4018/978-1-7998-2466-4.ch063

Caspary, K., & Warner, M. (2016). What it takes to create linked learning: A report on lessons learned from evaluating the approach in practice. SRI International.

Choudhury, M. D. (2022, January 12). Shortage of cybersecurity professionals a key worry for firms in '22. Mint. https://www.livemint.com/technology/shortage-of-cybersecurity-professionals-a-key-worry-for-firms-in-22-11642015098080.html

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a Time: A systematic review of cybersecurity digital games. Simulation & Gaming, 51(5), 586–611. https://doi.org/10.1177/1046878120933312

Coleman, C. D., & Reeder, E. (2018). Three reasons for improving cybersecurity instruction and practice in schools. In E. Langran & J. Borup (Eds.), Proceedings of Society for Information Technology & Teacher Education International Conference (pp. 1020-1025). Association for the Advancement of Computing in Education. http://www.learntechlib.org/p/182648/

Domeij, T. (2019). K-12 cybersecurity program evaluation and its application [Bachelor's project, Bridgewater State University]. Virtual Commons. https://vc.bridgew.edu/honors_proj/366

Drmola, J., Kasl, F., Loutocký, P., Mareš, M., Pitner, T., & Vostoupal, J. (2021). The matter of cybersecurity expert workforce scarcity in the Czech Republic and its alleviation through the proposed qualifications framework. The 16th International Conference on Availability, Reliability and Security, 143, 1-6. https://doi.org/10.1145/3465481.3469186

Dunn, M. H., & Merkle, L. D. (2018, February). Assessing the impact of a national cybersecurity competition on students' career interests. Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 62-67). https://doi.org/10.1145/3159450.3159462

Filipczuk, D., Mason, C., & Snow, S. (2019). Using a game to explore notions of responsibility for cyber security in organisations. Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, 1-6. https://doi.org/10.1145/3290607.3312846

Finch, A., Burrell, D. N., Lu, S., Dawson, M., Springs, D., Bilberry, K., Anderson, D. P., & Modeste, R. (2020). Cybersecurity workforce development in minority, low income, and native American reservation communities. International Journal of Smart Education and Urban Society, 11(4), 35–52. https://doi.org/10.4018/IJSEUS.2020100103

Fourie, L., Sarrafzadeh, A., Pang, S., Kingston, T., Hettema, H., & Watters, P. (2014). The global cyber security workforce – An ongoing human capital crisis. Global Business and Technology Association, 173-184. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.940.6951&rep=rep1&type=pdf

Garba, A., Maheyzah, B. S., Siti, H., & Ibrahim, B. D. (2020). Cyber security awareness among university students: A case study. Science Proceedings Series, 2(1), 82–86. https://doi.org/10.31580/sps.v2i1.1320

Giboney, J. S., McDonald, J. K., Balzotti, J., Hansen, D. L., Winters, D. M., & Bonsignore, E. (2021). Increasing cybersecurity career interest through playable case studies. TechTrends, 65, 496-510. https://doi.org/10.1007/s11528-021-00585-w

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hasib, M. (2018). Cybersecurity as people powered perpetual innovation. In Information technology-New generations (pp. 7-10). Springer, Cham.

Hodhod, R., Khan, S., & Wang, S. (2019). CyberMaster: An expert system to guide the development of cybersecurity curricula. International Journal of Online and Biomedical Engineering (IJOE), 15(03), 70-81. https://doi.org/10.3991/ijoe.v15i03.9890

Javidi, G., & Sheybani, E. (2018). K-12 cybersecurity education, research, and outreach. 2018 IEEE Frontiers in Education Conference (FIE), 1-5. https://doi.org/10.1109/FIE.2018.8659021

Jayakumar, P., Brohi, S. N., & Zaman, N. (2020). Top 7 lessons learned from COVID-19 pandemic. TechRxiv. (Preprint). https://doi.org/10.36227/techrxiv.12264722.v1

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning, 12(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. (Preprint). https://doi.org/10.36227/techrxiv.12278792.v1

Moallem, A. (2019). Cyber security awareness among college students. In T. Ahram & D. Nicholson (Eds.), Advances in Human factors in cybersecurity (pp. 79–87). Springer. https://doi.org/10.1007/978-3-319-94782-2_8

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human. Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, 157–176. https://doi.org/10.1145/3344429.3372507

Nobles, C. (2018). The cyber talent gap and cybersecurity professionalizing. International Journal of Hyperconnectivity and the Internet of Things, 2(1), 42–51. https://doi.org/10.4018/ijhiot.2018010104

Oyedotun, T. D. (2020). Sudden change of pedagogy in education driven by COVID-19: Perspectives and evaluation from a developing country. Research in Globalization, 2, 100029. https://doi.org/10.1016/j.resglo.2020.100029

Pati, D., & Lorusso, L. N. (2018). How to write a systematic review of the literature. Health Environments Research & Design Journal, 11(1), 15–30. https://doi.org/10.1177/1937586717747384

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student perceptions of challenges and role of mentorship in cybersecurity careers: addressing the gender gap. Information Systems Education Journal, 18(3), 44–53. https://files.eric.ed.gov/fulltext/EJ1258205.pdf

Sanzo, K. L., Paredes Scribner, J., & Wu, H. (2021). Designing a K-16 cybersecurity collaborative: Cipher. IEEE Security & Privacy, 19(2), 56–59. https://doi.org/10.1109/msec.2021.3050246

Smith, D. T., & Ali, A. I. (2019). You've been hacked: A technique for raising cyber security awareness. Issues In Information Systems, 20(1), 186–194. https://doi.org/10.48009/1_iis_2019_186-194

Smith, G. (2018). The intelligent solution: Automation, the skills shortage and cyber-security. Computer Fraud & Security, 2018(8), 6–9. https://doi.org/10.1016/s1361-3723(18)30073-3

Srivatanakul, T., & Annansingh, F. (2021). Incorporating active learning activities to the design and development of an undergraduate software and web security course. Journal of Computers in Education, 9(1), 25–50. https://doi.org/10.1007/s40692-021-00194-9

Stoker, G., Clark, U., Vanajakumari, M., & Wetherill, W. (2021). Building a cybersecurity apprenticeship program: early-stage success and some lessons learned. Information Systems Education Journal, 19(2), 35–44. https://files.eric.ed.gov/fulltext/EJ1297604.pdf

Tobarra, L., Utrilla, A., Robles-Gómez, A., Pastor-Vargas, R., & Hernández, R. (2021). A cloud game-based educative platform architecture: The cyberscratch project. Applied Sciences, 11(2), 807. https://doi.org/10.3390/app11020807

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. Computer Fraud & Security, 2019(5), 9–12. https://doi.org/10.1016/s1361-3723(19)30052-1

Wright, M. A. (2016). Improving cybersecurity workforce capacity and capability. ISSA Journal, 14–20. https://cupdf.com/document/improving-cybersecurity-workforce-capacity-and-capability.html

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. IET Software, 13(2), 159-169. https://doi.org/10.1049/iet-sen.2018.5095