8-2024

Cybersecurity in Education

Rahima Shelim

ABSTRACT

Cybersecurity is becoming increasingly important as we rely more on digital devices and programs to conduct our daily lives, including the transfer and storage of personal information. According to research, one of the most critical stages in improving cybersecurity is to implement an effective security awareness program. In this work, we seek to understand the existing level of security knowledge among college students, industry professionals and create a module to help raise the awareness. Our module's primary elements are interaction and the display of alarming effects of reckless cyber behaviors among common Internet/technology users. This report presents a simple systematic literature analysis to examine the current position on cybersecurity education. In our study, we evaluated and studied 25 research articles and publications that we deemed to be the most relevant to the subject in order to extract and derive useful material with instructional and practical value to cybersecurity education.

We designed a survey and interviewed 4 industry experts who are currently working in the cybersecurity field. More than 100 people participated in our survey and the results indicated that the majority of the respondents are either non-cybersecurity majors or had not enough hands-on experience in cyber security. It has raised a red flag for the future generation of our country. As a result, we have designed a course based on the research, industry review and survey respondents on what needed to be done to raise awareness and motivate students to pursue a career in cybersecurity.

Keywords: Cybersecurity, cyber safety, cyber education, cyber awareness

MONTCLAIR STATE UNIVERSITY

Cybersecurity in Education

By

Rahima Shelim

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

August 2024

College: College/School: Science and Mathematics

Thesis Committee:

Department: Computer Science

[redacted]_____

Dr. Kazi Sultana

Thesis Sponsor

[redacted]__________

Dr. John Jenq

Committee Member

[redacted]

Dr. Boxiang Dong

Committee Member

CYBERSECURITY IN EDUCATION

A THESIS

Submitted In Partial Fulfillment of the Requirements

For the Degree of Master of Science

By

RAHIMA SHELIM

Montclair State University

Montclair, NJ

2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

First and foremost, I would want to sincerely thank and appreciate my advisor, Dr. Kazi Sultana. She has been an amazing mentor, and I am very grateful for having her inspired me and assisted me in organizing my ideas. Additionally, I want to thank my committee members Dr. John Jenq and Dr. Boxiang Dong for supporting my research and helping me develop my research skills. Their guidance on how to finish my master's program and on research techniques has been essential.

I would like to thank a very special person who holds my heart firm is my mom. Her encouragement and understanding throughout my master's program allowed me to continue my education. I'm also grateful to my brother, who has always been the brightest part of my life and has inspired and motivated me to get things done.

Above all, I want to express my gratitude to my family for their love and support throughout the years. Not but least, I have been fortuned enough to have an ever-supportive father who has always encouraged me to pursue my goals. I want to express my gratitude to him for always having faith in my ability to succeed in life as well as in the academic area.

CHAPTER 1

INTRODUCTION

Education is no longer limited to traditional classrooms in today's digital world. The incorporation of technology into educational processes has created limitless possibilities, but it has also exposed educational institutions to cybersecurity dangers. Education's cybersecurity has become critical, as educational institutions hold massive amounts of sensitive data such as student records, financial information, and intellectual property. Furthermore, cyber threats can interrupt learning settings, halting academic activity and resulting in severe financial losses.

Cybersecurity is one of the most in-demand skills for Information Systems graduates, making it crucial to the Information Systems curriculum. There is a significant shortage of qualified cybersecurity graduates. It is anticipated that there would be a global shortage of nearly 3.5 million cybersecurity specialists by 2025. Organizations are having difficulty filling security personnel. According to Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), firms are having difficulty filling cybersecurity positions, posing a risk to national security. [4]

Developing training programs that incorporate effective theoretical learning frameworks adapted to meet industry goals is difficult. Previous research has shown outcome-based educational systems as an effective strategy to teaching and learning. [9] This strategy prioritizes the targeted results or objectives that students should achieve by the course's end. These educational objectives determine the course material, teaching methods, and evaluation systems.

Backward course design, a method of outcome-based educational design, is a deliberate and focused approach to instructional course design that requires a fundamental shift in education. This transition requires first considering the learning objectives before designing the teaching and learning activities. [10] [18]

To address this shortage, the research proposes strategies for promoting cybersecurity education in schools, including integrating cybersecurity topics into existing curriculum subjects, organizing cybersecurity awareness events, and establishing cybersecurity organizations or clubs, aiming to prepare students to fill the cybersecurity talent gap; who can meet the industry demands. [10]

The motivation of this paper is to look into the development of a cybersecurity curriculum that effectively integrates technical, professional, and theoretical elements to meet industry needs while also cultivating enthusiasm and engagement among students interested in pursuing a career in cybersecurity. The objectives are as follows:

- Design a course strategy to organize the cybersecurity curriculum.
- Ensure that the course content is aligned with the industry's cybersecurity demands in order to offset the lack of cybersecurity expertise.
- Increase students' interest in entering the cybersecurity sector.

The cybersecurity course, along with other courses in the concentration, aims to provide graduates with the skills required to meet the current need in the cybersecurity sector. However, there has been a lack of prior research that precisely addresses the theoretical foundation required for building a cybersecurity course that meets industrial needs. To approach the current state of cybersecurity education, we conducted a basic systematic literature review. Secondly, we conducted a literature review on '25' research articles and publications that we deemed to be of the highest relevance to the subject. Finally, we proposed a survey and interviewed four industry professionals who are currently or have previously worked in the cybersecurity sector, after which we built a course to attract students to the cybersecurity field.

The remainder of the paper is organized as follows: In Chapter 2, we offer our initial research questions, and survey methodology. In Chapter 3, we included a brief overview of each selected paper based on the research questions. In Chapter 4, we present our survey design, an overview of our interview summary with industry experts. In Chapter 5, we discussed our findings from the survey participants and thoughts. In Chapter 6, we wrap up our work and outline our future goals.

CHAPTER 2

METHODOLOGY

2.1 Research Questions

This paper aims to conduct a literature survey to identify the volume and usage of current research on cybersecurity education. The initial search goal was to gather relevant documents for subsequent examination and analysis. We established the following research questions below to guide our search strategy and paper collecting. We will refer to these as IRQ (Initial Research Questions) to distinguish them from the research question that will be derived in the next step.

IRQ1: What is the current state of the art of cybersecurity education?
IRQ2: What areas of knowledge are currently being focused on in cybersecurity education?
IRQ3: What valuable information about cybersecurity education may be used or given to students or can be presented to the students?

The purpose of these listed questions to improve the search strategy and support the reverse engineering process. In this context, reverse engineering refers to the process of refining research questions based on the information gathered from literature surveys and paper evaluation.

2.2 Data Statistics

An electronic search was conducted in order to collect research articles on specific digital libraries that we considered to be popular and more frequently visited by scholars nowadays.

Table I summarizes the results of our initial search utilizing the query keyword and exclusion criteria on selected digital libraries. To find papers and publications on cybersecurity education, we specified our exclusion criteria as follows:

- Exclude books, book chapters, abstracts, summaries, and notes. This category includes presentations, technical reports, and grey literature (not published in a journal or conference).
- Exclude publications dated before 2010.
- Exclude papers that are not written in English (including translations).

Library	**Query Results**	**Filters**
ACM Digital Library	3,257	− Research Article − 2010 - 2024
IEEE Computer Society Digital Library	2,873	− Conference publications − Journals − 2014 - 2024
ScienceDirect	4,301	− Research Article − 2014 - 2024
Google Scholar	17,504	− 2014 – 2024 − Not including citations
Springer Link	2,765	− Article − 2012 – 2024 − English

TABLE 1: PRELIMINARY SEARCH RESULT ON SELECTED LIBRARIES

After following the search technique, making the final number of papers surveyed in this work “25” published research papers and articles.

2.3 Paper Collection

After following the search technique outlined in the previous stage (2.2 Data Statistics). We used a simple filtering strategy. The first step was to read the titles of the top "30" relevant records retrieved by applying the search term on each library (total of "100" titles), assess which publications are more favorable to the topic of cybersecurity education, and exclude any papers that were duplicated or falsely retrieved while within the exclusion criteria. This filtering step yielded "40" titles.

The next stage was to scan the abstracts and headers of the selected "40" articles to see if the material presented is relevant to cybersecurity education. This step decreased the overall number of papers to 25. The scanned papers underwent "full-text" evaluation to assess the feasibility of synthesizing and evaluating specific research topics and replies. Consider whether the paper includes definitions, characteristics, current status, causes, or resolution for cybersecurity in education. This effort surveyed 25 published research papers and articles.

CHAPTER 3

LITERATURE REVIEW

3.1 Paper Analysis

After analyzing and evaluating the finalized papers, we can identify the research questions that are being addressed and explored in the selected publications. This literature review is evaluated based on its capacity to give satisfactory responses to the research questions posed. The analysis of chosen papers raised the following research questions:

RQ1: What is the importance of cybersecurity education?

RQ2: What are the strategies that schools/government uses to promote cybersecurity education?

RQ3: What are the current/ future organizational needs in the Cybersecurity field? What challenges & privacy threats concerning students, educators, and schools/government towards cybersecurity?

The selected papers were reevaluated to determine their relevance to the study questions. The purpose of this research is to evaluate the literature's ability to provide acceptable answers to such common scholarly inquiries. After analyzing chosen papers, the following research topics were identified:

RQ1: What is the importance of cybersecurity education?

Many of us use social media to express our feelings, share thoughts, gain popularity or to become known. Many of us want to be the first to share an issue; but we often disregard the authenticity of the information [1]. Cybersecurity education is crucial for adults specially children in today's technology-driven world. Excessive Internet use might pose cyber hazards, despite its possible benefits.

Access to the internet is continuing to rise, along with the need for a variety of purposes. According to the National Level Evidence based results by the top professionals from the United States, United Kingdom, & South Africa present quantitative findings of empirical evidence support the effectiveness of CEAT efforts in 80 countries. The research discusses the importance of cybersecurity education, awareness, and training (CEAT) in light of the expanding use of the internet and rising cyber threats. It highlights that despite the widespread internet use, many individuals lack awareness of cybersecurity risks and have never received formal training. By one estimate, the global costs of cybercrime are expected to exceed $10.5 trillion per year by 2025, underscoring the urgent need for effective CEAT programs. [2]

The impact of CEAT initiatives on internet use and services at the national level, using data from 80 nations. It identifies positive correlations between CEAT and internet vitality, suggesting that effective CEAT programs contribute to improved cybersecurity and internet usage. However, many nations, particularly low-income ones, have limited maturity levels in CEAT initiatives, indicating the need for further investment and development in this area. [2]

The qualitative analysis is based on a subset of CMM (Cybersecurity Capacity Maturity Model) reviews conducted in 23 countries across Europe, Africa, and the Oceania region. The analysis includes additional countries to ensure a comprehensive view. Several challenges to the development of CEAT (Cybersecurity Education, Awareness, and Training) were identified:

- Lack of coordinated national cybersecurity awareness programs. [11] [18]
- Limited awareness at the executive or board level regarding cybersecurity risks. [16]
- Inadequate national budget allocations for cybersecurity education. [19]
- Shortage of qualified educators in cybersecurity. [14]
- Migration of skilled cybersecurity professionals. [15]
- High cost of professional cybersecurity certificates. [14]
- Lack of knowledge transfer across nations. [13] [10] [17]
- Language barriers. [14]

With the widespread adoption of the internet, social media, and mobile smartphones, individuals are increasingly burdened with greater responsibilities. While many internet users are informed enough to protect themselves and others [2], many are still unclear of how cyber-attacks occur or how to defend against them. For example, a poll of US households found that while 75% of respondents could identify a strong password, just 13% knew the function of a virtual private network (VPN), and only 10% recognized an example of multi-factor authentication. As a result, it is very important to study cybersecurity for professional and personal life. [12]

This lack of awareness about basic security procedures highlights the need for improved educational programs, more awareness, and more cybersecurity training options worldwide. Because of, several long-term national initiatives have been launched, including those by the Computer Science and Telecommunications Board (CSTB) in the United States and the National Cyber Security Centre in the United Kingdom, to investigate the potential of national-scale efforts. [21]

RQ2: What are the strategies that schools/government uses to promote cybersecurity education?

The critical role of digital information and telecommunication technologies in individuals' lives and a nation's economic growth, societal well-being, infrastructure resilience, and national security. It emphasizes the importance of cybersecurity education in fostering a resilient cybersecurity ecosystem and supporting national cyber sovereignty. The study [2] reviews the National Cybersecurity Strategic Plans (NCSPs) of leading countries and examines existing cybersecurity education improvement initiatives. It proposes adopting the Goal-Question-Outcomes (GQO)+Strategies paradigm to align cybersecurity education programs with national strategic goals, mapping cybersecurity skills and competencies using the National Initiative for Cybersecurity Education (NICE) framework. The proposed curricula align with three major cybersecurity strategic goals: developing secure digital infrastructure, defending against cyber threats, and enhancing cybersecurity awareness. The study suggests that cybersecurity university programs use the GQO+Strategies paradigm to bridge skill gaps and support national cybersecurity workforces. [2] [3] [17]

On the other hand, The European Union Agency for Cybersecurity (ENISA) Programs presents an analysis of the Cybersecurity Higher Education Database (CyberHEAD) to assess the state of cybersecurity skills supply in the European Union (EU). The increasing number and impact of security incidents, accelerated by the digital transformation accelerated by the COVID-19 pandemic, have highlighted the need for robust cybersecurity measures. [14]

Since 2016, the EU has implemented minimum legal requirements for essential service operators and adopted national cybersecurity strategies to enhance cyber resilience. However, the demand for cybersecurity professionals has outpaced supply, leading to a significant skills gap. To address this gap, initiatives such as the European Cybersecurity Skills Framework and the European Commission's Cybersecurity Skills Academy have been developed. [14] [17]

ENISA's CyberHEAD database, launched in 2020, serves as a repository of higher education programs in cybersecurity offered by institutions across the EU and European Free Trade Association (EFTA) countries. The database, consisting of 142 cybersecurity programs from 26 EU and EFTA countries, aims to provide insights into the state of higher education in cybersecurity and help bridge the skills gap. Programs listed in CyberHEAD must meet specific criteria regarding accreditation, cybersecurity content, and regular updates to ensure relevancy. [1] [14]

The European agency did a comparison between enrollment data for 2020 and 2021 reveals a 20% overall increase in enrollments and a 23% increase in female enrollments, indicating a growing interest in cybersecurity-related programs and jobs. However, while enrollment numbers have risen, the total number of graduates in 2021 only saw a small 2% increase overall, with a notable 22% increase in female graduates. [14]

A survey [1] conducted to understand why students drop out or delay their studies identified several key reasons:

- Many students are already working or find jobs while studying (43% of responses).
- Some find the program curricula too demanding (12%).
- Dissertation requirements take longer than anticipated (12%).
- The COVID-19 pandemic caused issues leading to dropouts or delays (9%).
- Other reasons include family obligations, postponement of studies, or career policies (24%).

While projections suggested a doubling of cybersecurity graduates in the next few years, data from CyberHEAD, a database of cybersecurity academic programs, indicates challenges in students completing their studies on time. About 36% of students in one-year programs don't graduate within the expected timeframe. However, many students who drop out or delay their studies still enter the cybersecurity workforce. [9] [13]

The transition from a physical classroom to a digital one during the COVID-19 pandemic was fraught with minimal resources, a technological knowledge gap, a lack of support from the government, and vast socioeconomic disparity. Nevertheless, many educational institutions could take on this task and execute it, albeit with some difficulties. The availability of technology and infrastructure to support such a massive move helped preserve the learning progress of many students. However, most families and educators across the US struggled to keep up with the online education format. Many parents, educators, and other caregivers who form the student support structure had to overcome network issues, technical errors, and limited knowledge of the platform to create an engaging virtual learning environment. For working parents, this was a tough task as they were forced to continue their work from home while overseeing their children. Online education was a challenging experience for educators and other caregivers as well. Similarly, students had to spend much of their time in front of the devices to receive education and interact with peers and, after that, had to invest more time trying to adjust to new learning formats. As most of the population was spending time online interacting with new technology platforms and tools, the target pool for cybercrime was at an all-time high. [9]

CyberHEAD serves as a valuable resource for students seeking cybersecurity programs and provides insights into the state of higher education in cybersecurity across the EU. It aims to help EU Member States make informed decisions and bridge the gap between professional workplace needs and academic learning environments. As 2023 is designated the Year of Skills in the EU, it's crucial for learners to understand career opportunities in cybersecurity and make informed decisions about their futures. [9] [14]

RQ3: What are the current/ future organizational needs in the Cybersecurity field? What challenges & privacy threats concerning students, educators, and schools/government towards cybersecurity?

- Language barriers

Language barriers play an important part in today's environment. Overcoming cybersecurity communication obstacles between cybersecurity professionals and non-technical users (e.g., government officials, firm senior executives, and the common citizen) remains difficult and causes a disconnect. Some CMM reports emphasized a lack of acceptable local language options for explaining new technical concepts to citizens, resulting in another linguistic barrier to the success of cybersecurity awareness raising programs. [5] [12] [19]

- Cybersecurity budgets

Even while including cybersecurity into the national curriculum is viewed as critical for developing cybersecurity skills and raising awareness throughout formal education systems [24], obtaining funding support to achieve these objectives is difficult. According to the CMM studies, many countries provided no or minimal resources for cybersecurity education and national curriculum due to resource and capability issues. As a result, there is frequently no established formal national curriculum for cybersecurity training or degrees. In unusual circumstances, the government, schools, and industry worked together informally to provide the resources required for CEAT. Given the rapid evolution and expansion of the cyber realm, academic institutions are battling to keep their courses current. [9] [24]

- Qualified educators in cybersecurity

Globally, demand for cybersecurity skills greatly exceeds the existing supply of traditionally trained professionals.[17] This issue was validated during the focus group talks for the CMM reports, which stated that the market requires technical and professional cybersecurity skills that are frequently unavailable through rigorous theoretical programs given by universities and other institutions. The universities claimed there are a shortage of certified cybersecurity educators/staff and a lack of competence in cybersecurity teaching. The research also revealed that women were dramatically underrepresented in cybersecurity, a problem that may necessitate university-level recruitment, outreach, and retention efforts. [11] [10] [14] [18]

- Privacy & Security Challenges

It is reported that during the COVID-19 pandemic, when most of the population relied upon online interaction to meet daily needs, the number of cybercrimes increased by 600%. Although these crimes might affect all users equally, the scope and impact of such crimes have increased dramatically among the vulnerable population like young students, the elderly, and so on. Thus, online education platforms and technical tools are paramount to be secure and privacy-preserving. However, the platforms widely utilized for online education worldwide were not explicitly designed to deliver education to hundreds of thousands of children and students in a secure way. Instead, these platforms and technologies were selected for their availability, ease of use, and ability to meet the requirements of a simulated classroom with minimum setup and time. [8] [9]

As a result, most of the population online was unfamiliar with these technological tools and lacked important cybersecurity knowledge. In July 2019, hackers held technology systems at Monroe College in NY at ransom for $2 million in bitcoin as reported in the news2. In a similar cyberattack incident, the Federal Bureau of Investigation notified Pearson, a British educational software, of a data breach that exposed sensitive information like names, date of births and email address of students from more than 13,000 school and university accounts. The pandemic has highlighted the need for cybersecurity education and awareness in the general population. Students, especially those under the legal age, are more vulnerable to online threats and attacks, as they are unable to understand the severity of cybercrimes and equally unable to prevent or resolve such attacks. The student support structure involving the parents, educators, and other caregivers is thus in a critical position to make decisions to safeguard the privacy and security of students. [9]

- The Need of Cybersecurity Education

Safety and security are semantically distinct concepts that require various levels of knowledge and skill. Smartphone users of all ages should be aware that their phones are vulnerable to attack and know how to increase device security. Because education is fundamental to security awareness and competence [11], cyber security education must reach all segments of society and people of all ages. [16]

Cyber security education consists of two components: first, people must be made aware of the need to take safeguards, and then teachers must implement the skills necessary to take those precautions. The article discusses the importance of raising awareness as a necessary prerequisite for learning cyber security skills. They focus on analyzing the levels of cyber security awareness of South African university students as developing nation citizens, which is the "outcome" of the larger South African cyber security educational strategy. Moreover, investigate if existing knowledge levels reflect the same gender discrepancy as seen in other socioeconomic sectors in South Africa. [16]

The article focused on smartphone cyber security in South Africa for three reasons: The first is that cyber-attacks are becoming more common, and developing countries are no exception [23]. Cyber criminals, realizing that large organizations are improving their cyber security and thus becoming more difficult to compromise, have shifted their focus to easier targets: small businesses and home computer users [24], both of whom do a lot of their computing on smartphones. [23] [24] [25]

The second reason is that smartphone ownership is growing worldwide, creating an attractive attack surface for hackers to target the unsuspecting or defenseless. Smartphone use has outpaced predictions, but regrettably, so have security flaws. A lack of knowledge and awareness is triggering the cyber-security problem. [22] South African smartphone ownership was 51% in 2018 [24], higher than global computer ownership [22], suggesting that South Africans may be more exposed to smartphone-enabled attacks than citizens of other nations. [23] [24]

The third reason is that South African children are increasingly buying and using smartphones. According to Business Tech [23], 80% of secondary school students in South Africa possessed a smartphone in 2017, whereas Porter [25] stated that 51% of elementary school students owned mobile phones. Because South African adolescents and youth are early adopters of new mobile technologies, and South African university students are heavy users of smartphones, we cannot wait until adulthood to raise security awareness and ensure that people have the necessary security skills. Students are strong consumers of technology, yet they do not often receive rigorous cybersecurity education. [21][23][25]

According to statistical records from the Cyber Crime and Multimedia PDRM Investigation Division, cyber-love scams, often known as the African Scam, are on the rise. Malaysia reported 1095 cases of cyber fraud in 2013, up from 814 cases in 2012. [19] Furthermore, according to [20], fraudulent online purchases surged in Malaysia in 2015, resulting in a loss of more than RM4.9 million across the automobile, housing, and tourism sectors. Cybersecurity education is also required to prevent computer game addiction. This addiction undoubtedly has harmful consequences. Teenagers spend a lot of time on computers and use their devices to socialize.

CHAPTER 4

SURVEY DESIGN

Designing a survey is a hard process in general and taking into account the best interests of all parties (institution, students, and industry) makes it even more complicated. Based on the research and findings we have designed a few interview questions and a survey to find out what's needed to promote cybersecurity in education. Our process for developing a very basic series of cybersecurity survey questions that are consistent with industry demands consists of raising cybersecurity awareness and attracting people into cybersecurity education. This will help to enhance security awareness among college students/institutions and industry on the use of the internet and its associated technologies. We believe that encouraging more individuals into cybersecurity, particularly women, will help to develop a safer cyber culture for us and future generations.The proposed cybersecurity questions design model consists of the following steps:

- To examine the pattern of security awareness and emphasize the crucial role cybersecurity plays in protecting personal, organizational, and national security interests.
- To identify the modules' efficiency in creating awareness among college students/institutions and industry.
- Develop educational content.

We have targeted college students, Institute, and Industry as our audience because of the following reasons:

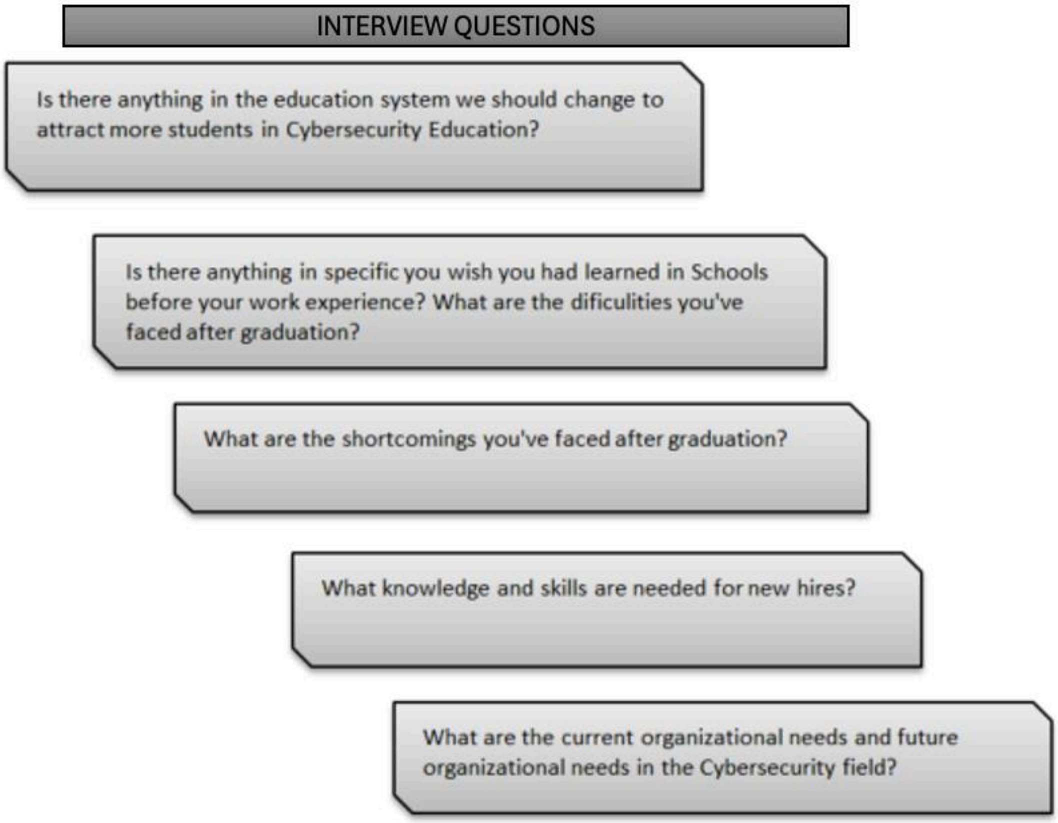
- Our audience relies on technology and the Internet for the three major activities such as education, socializing, and work.
- College students are the future workforce, future teachers, and parents. The impact of their security aware behavior will be significant and far reaching for the society that is why it is very important to invite more people in the cybersecurity field.

The main focuses of this survey are:

- The survey focuses on the fact that our audience can provide insights into areas where further education and support may be needed.
- The most common vulnerabilities people make such as weak password, lack of awareness, and risky browsing habits.

4.1 Interviews with Industry Experts

In addition to the insights gathered from the literature review and industry reports, we conducted interviews with four leading cybersecurity professionals, each with over five to ten years of experience. The interviewees included the COO & Co-Founder of BLAKFX (Kara), a project manager from KMBS (Ivan), a representative from a nonprofit government organization in the east (Kadian), and a SOC Analyst at Summit 7 (Picone). These interviews aimed to gain a deeper understanding of what cybersecurity organizations seek in new hires and their industry requirements. We asked about current security needs and trends, future security goals, and the preferred or required qualities for job candidates at US security organizations. The interviews were guided by semi-structured questions and each lasted approximately 30 minutes. Table 3 summarizes the compiled answers, with the key findings outlined below. Survey questions for the interview with top professionals shown below in Table 2.



INTERVIEW QUESTIONS

Is there anything in the education system we should change to attract more students in Cybersecurity Education?

Is there anything in specific you wish you had learned in Schools before your work experience? What are the dificulities you've faced after graduation?

What are the shortcomings you've faced after graduation?

What knowledge and skills are needed for new hires?

What are the current organizational needs and future organizational needs in the Cybersecurity field?

TABLE 2: INTERVIEW QUESTIONS FOR INDUSTRY EXPERTS

Questions Topic	Answers Summary
Things that would attract more students in Cybersecurity Education:	• Hands-on training with networking equipment and labs would make students very attractive. (Kara, Ivan, Picone, Kadian) • Hands-on cybersecurity experience from internships, part-time job opportunities, or lab work. (Kara, Ivan) • To support individuals at both professional and awareness levels, facilitating their exploration of cybersecurity topics and guiding them towards suitable educational opportunities to enhance their skills in the cybersecurity field. (Ivan, Kara) • Provide assistance and support in navigating the educational landscape, including information on scholarships, financial aid, and professional development possibilities. (Picone) • Create scenarios in which students must evaluate digital evidence from many sources, including hard drives, network traffic, and mobile devices. They can learn how to recover data, analyze logs, and detect cyber threats. (Picone, Kadian) • Provide clear pathways and resources for anybody interested in pursuing cybersecurity education, including information on relevant

	courses, certifications, training programs, and career opportunities. (Kadian)
Problem faced:	• The lack of clarity regarding qualifications has resulted in many job holders lacking the necessary training and professional qualifications to fulfill the demands of their positions. As some of the cybersecurity certifications are prohibitively expensive therefore many candidates are self-educated. (Kara) • Teachers lack knowledge. (Kara, Ivan) • The lack of resources and access to learning materials and facilities to implement cybersecurity education. (Ivan) • I wish I had gained real world experience through internships or by volunteering in non-profit organizations. (Ivan) • I didn't learn much in college so I did a certification program through a bootcamp. (Picone)
Problem faced at work:	• Didn't have enough hands-on experience so it was tough in the beginning. (Ivan) • Didn't have certifications and the employers

	are more comfortable with hiring candidates with a few years of experience. (Kara) • I had to do a bootcamp and multiple certificate programs to land a job. (Picone)
Knowledge and skills needed for the new hires:	• We value candidates with CCNA and CISSP certificates. (Kara) • We are looking for someone who can understand important business requirements and apply them to coherent cybersecurity policy. (Kara, Ivan) • We need people that understand risk management and network architecture from a business viewpoint, are capable of asking essential questions, and can configure networks to maximize critical company activities. (Picone) • Hands-on experience is preferred, supplemented by necessary courses, and industry certifications are beneficial in the recruitment process. (Kara, Ivan) • Understanding the OSI model, TCP/IP operations, and packet transport across the Internet is critical. (Kara) • It is critical to recognize the importance of supporting the business and its users. (Kadian, Ivan)

	• Understanding legal and regulatory compliance, as well as the non-technical components of cybersecurity, is vital. (Ivan, Picone)
Current Organizational Needs in the Cybersecurity field:	• Raising awareness and education are extremely essential underlying principles and complements to everything that the government and industry undertake. (Picone) • Almost all of our networking and cybersecurity technologies are built on Cisco technology. We require folks with Cisco experience. (Ivan) • We outsource much of our cybersecurity work to Cisco due to a lack of competent candidates. (Ivan) • We need to hire people who have hands-on experience with Cisco equipment and security programming. (Ivan) • We are seeking cybersecurity professionals for analytic, policy, risk management, and networking roles. Our hiring mix is approximately 65% technical - security engineers, architects, pen testers, incident handlers - and 35% management - governance, risk, and compliance focused. (Kara)

	• Companies and organizations must realize that, regardless of the level of protection or cybersecurity investments they undertake, the chance of a breach is always present, given the ever-changing cyber threat landscape. As a result, it is critical to consider how to detect, respond to, and recover from the breach as quickly and smoothly as feasible. (Picone, Kadian) • Someone who is excited to work in the cybersecurity field. (Ivan, Kara, Kadian)
Future Organizational Needs in the Cybersecurity field:	• We require people who are interested in staying with us and have understanding of security and networking, as well as hands-on abilities. The industry is extremely competitive for qualified cybersecurity professionals. Most cybersecurity professionals can change employers every 16-18 months and significantly boost their compensation. (Kara) • Recruiting dedicated cybersecurity professionals. It is difficult to discover strong cybersecurity hires who will stay for more than two years. (Ivan) • We require individuals who are open and dedicated to continuous development. The

	field of cybersecurity is expensive and constantly evolving. New legislation and standards are frequently introduced, particularly in the governance, risk, and compliance areas. On the technical level, threat actors are always discovering new ways to breach systems, and new technologies are being developed to mitigate and protect against these threats. (Kara) • The world could be considerably more secure if governments, industry, and citizens immediately undertake the appropriate measures. (Picone, Kadian) • Governments should use their procurement power to mandate more cybersecurity in their purchases, thereby setting a positive example. Industry should continue to work collaboratively to develop new cybersecurity standards and raise the bar. (Picone)

TABLE 3: SUMMARY OF INTERVIEWS

CHAPTER 5

FINDINGS AND DISCUSSIONS

Here, we provide our study's findings. We will first give a brief summary of the demographics of our participants, and then we will discuss the survey's quantitative analysis. Lastly, we offer the analysis of the open-ended question evaluation from the survey or interview.

5.1 Demographics

A total of 100 participants took our survey on Google Forms. These included 37% participants who identified as students, 57% employed, and 3% as either unemployed or did not answer. 31% of our participants were aged between 25 to 30 years old. In addition, over 50% of our participants reported identifying as female, 48% identified as male, and the rest preferred not to answer. Finally, most participants (56%) reported at least bachelor's degree with having the highest percentage. Table 4 provides the overview of the participants' demographics of the study.

Age	Percentage
Less than 18 years	25.2
18-24 years	23.4
25-30 years	31.8
31-40 years	16.8
41-50 years	2.8
51-60 years	Did not answer
61-70 years	Did not answer

More than 70 years	Did not answer
Gender	
Female	50.5
Male	47.7
Transgender	Did not answer
Do not wish to specify	1.9
Education Level	
Less than high school	12.1
High school graduate	21.5
Bachelor's degree program	56.1
Master’s degree program	9.3
Other. (Please Specify)	0.9
Occupation	
Employed	57.9
Unemployed	3.7
Student	37.4
Retired	Did not answer
Do not wish to specify	Did not answer

TABLE 4: DEMOGRAPHICS OF THE PARTICIPANTS, INCLUDING AGE, GENDER, EDUCATION LEVEL & OCCUPATION

5.2 Importance of Cybersecurity

Figure 1 and Figure 2 result indicates the importance of cybersecurity. We asked our participants how important they feel of cybersecurity or safety. Most participants who took the survey 42% think cyber safety is “Very Important”, while 28% believe cybersecurity is “Moderately Important”. Only 6 participants proclaimed that cybersecurity is not essential. Our participants were asked whether they attended in any in cybersecurity awareness campaigns or workshops hosted by their educational institution. 73% participants never attended and 26% responded they did. We’ve also asked whether they received any formal cybersecurity training or education before. Over 81% of our participants never received formal cybersecurity training or education within the past year, only 18% received. Furthermore, the participants were asked how confident they are in terms of understanding basic cybersecurity principles and best practices. More than 45% of our participants deemed “Moderately Confident” in terms of understanding the basic cybersecurity principles and 30% said “Slightly Confident”. This can confirm the importance of cybersecurity education in raising future generation.

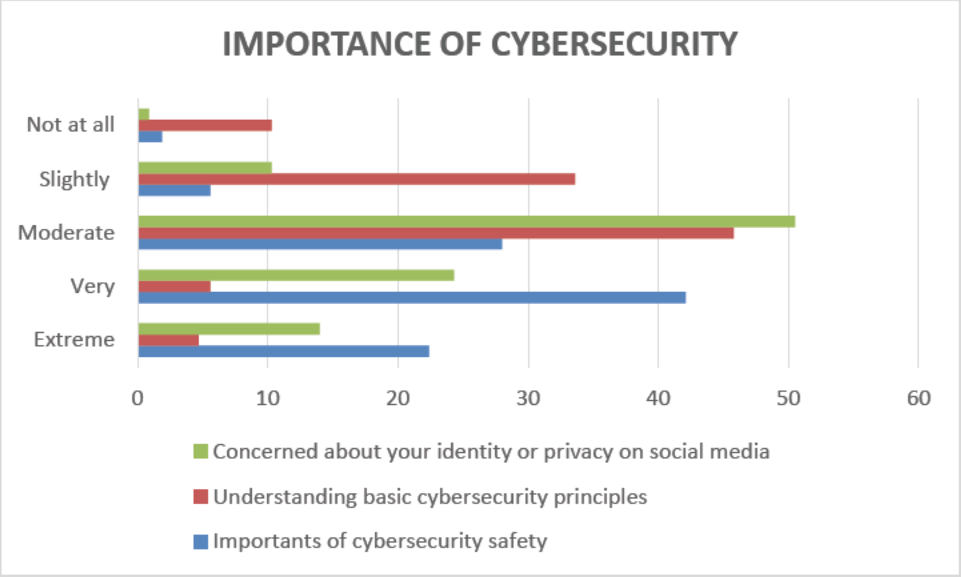


FIGURE 1: CYBERSECURITY IMPORTANCE AMONG PARTICIPANTS

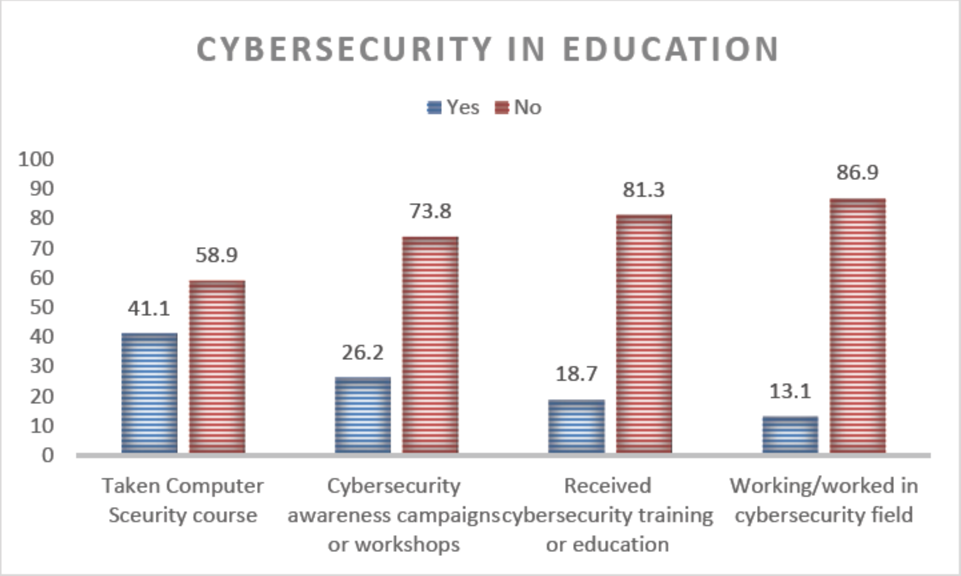


FIGURE 2: PARTICIPANTS IN CYBERSECURITY EDUCATION

5.3 Open-Ended Question Evaluation

We included a number of open-ended questions in our questionnaire to allow participants to share their ideas, opinions, and observations about the significance of cybersecurity for students. Participants in the survey section answered twelve questions, while each industry expert segment had five open-ended questions. Participants in the survey were not compelled to respond to any questions, therefore it stands to reason that they either rarely responded the text entry questions or gave brief or useless responses. However, more detailed responses show our participants' concerns and assumptions regarding the cybersecurity in the interview section. A few responses included a brief overview of important topics related to privacy communication, cybersecurity, and cyber safety, along with the difficulties associated with online learning.

Organizations continue to struggle to find graduates with the necessary skills they need. They feel that having a degree does not guarantee that an applicant is qualified for the job. More than 70% of cybersecurity firms estimate that more than half of graduates lack industry-specific skills. Only 27% of industry professionals believe that recent cybersecurity graduates are adequately qualified. The primary issue areas indicated by the industry review and survey are as follows:

- Cybersecurity requires soft skills (70 percent)
- IT knowledge and skills gaps required for cyber security (65 percent)
- Insufficient business insight for cybersecurity (55 percent)
- Technical Experience (65 percent)

- Insufficient hands-on training in cybersecurity (70 percent)
- Hands-on experience (70-80 percent)

The industry analysis and survey emphasized that technical abilities are the most important factor that employers examine when deciding whether a cybersecurity candidate is qualified. We must find the right balance of theory and hands-on expertise. The primary concern expressed by industry reviewers and survey respondents was a lack of hands-on experience and raising awareness. Industry experts believe that enhancing student motivation, self-efficacy, and engagement could be more useful. As a result, additional research is needed on this strategy in terms of student perception, like, and preference.

However, one of the key concepts is that it encourages deeper learning through hands-on experiences. It enables teachers to give online instructional videos, presentations, and other materials that students may learn and refer to at their own speed and from any time and location that is convenient for them. This strategy is better suited to individual learning demands than typical class lectures, which may be too quick for some while boring others. Furthermore, class time can be used more effectively by accommodating students' demands, such as labs, support sessions, and discussions.

In the field of cybersecurity, hands-on security analysis and response simulation activities are very effective in helping students to organize their conceptual knowledge in ways that facilitate retrieval and application. When students obtain basic knowledge through online lectures, their classroom time may be spent expanding their understanding and practicing their cybersecurity abilities.

Social networking sites including Facebook, Instagram, LinkedIn, YouTube, and Twitter are the most popular internet applications among students. This explosion of public information increases the potential of privacy and security breaches. The validity and accuracy of information in this virtual world might likewise be questioned. Children must be prepared to defend themselves and accept responsibility when confronted with potential cyber hazards. However, there are issues in ensuring that instructors are adequately qualified and up to date in their abilities to foster critical understanding rather than restrictive approaches to cyber safety, as well as assisting students and parents in their home internet use.

The numerous problems that schools encounter when implementing cybersecurity instruction include a lack of expertise, funds, and resources. Teachers have insufficient knowledge and skills in online. Schools and government agencies may not have the necessary resources or facilities to implement cybersecurity instruction. The rapid pace of technological change creates new risks, necessitating the development of innovative, secure solutions. This is a significant challenge for instructors since they lack access to learning materials and must be adaptable to technological development. Symposiums on cybersecurity should increase early exposure and training for students in schools. People who have been exposed to and trained in cybersecurity are projected to be the country's future sources of cyber defense.

5.4 Course Design

In this section we've designed a course. The aim of the course is to attract individuals to cybersecurity education: Attracting people to cybersecurity education involves emphasizing the importance of cybersecurity skills, showcasing the diverse career opportunities available, and providing engaging and accessible learning experiences.

This course provides a detailed examination of cybersecurity fundamentals, including important concepts, principles, technologies, and practices for securing digital assets, protecting privacy, and reducing cyber threats. Students will gain practical and theoretical understanding to better understand cybersecurity threats, tactics, and countermeasures in a range of computer environments. Table 5 shows the course design model. The course emphasizes hands-on exercises, case studies, and real-world scenarios to improve learning outcomes and prepare students for careers in cybersecurity.

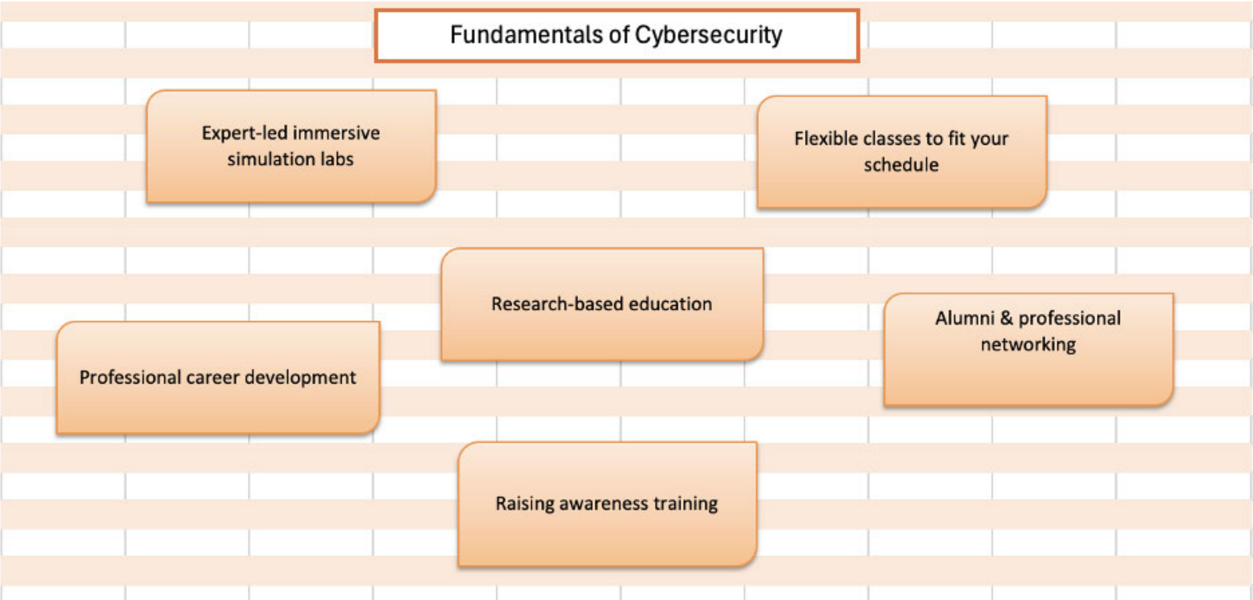

Fundamentals of Cybersecurity
Expert-led immersive simulation labs
Flexible classes to fit your schedule
Research-based education
Alumni & professional networking
Professional career development
Raising awareness training

TABLE 5: COURSE DESIGN MODEL

Based on the research, expert interviews and a survey, we've determined that if we have the above options available for the students, we will be able to attract more people in the cyber field. As we already know there are schools/universities do offer flexible class schedule, labs, and offer career opportunities such as workshop, seminar, and awareness programs etc. However, it's not enough for in today's tech world we should be more extensive about it. About 70% of the survey participants said we need more hands-on training incorporate with real world incidents. The current education systems do not offer enough lab works also any options for certificate in undergrad. They have earned certificates through boot camp. This makes student paying double in order to land a job because majority of the companies hire people with certificate. Which is leading students either drop out or doing boot camp instead of getting bachelor because it's much cheaper; but then there are companies that wouldn't hire without a bachelor degree which is making people miserable. It is very important for education systems to create a supportive learning environment for all students.

Flexible Learning Options: This course will be offered both online and in-person. Each unit is designed to cover approximately 2 to 3 sessions in a 16-week, one-semester, 3-credit hour course. All tasks, including case studies, projects, and labs, are spread out over the 16-week curriculum. The course also provides alternatives such as online courses, part-time programs, evening classes, and self-paced learning modules.

Expert Led labs: Provide students with hands-on learning opportunities in which they can apply theoretical information to real-world settings. To improve skills and problem-solving abilities, cybersecurity education should incorporate labs, simulations, and real-world case studies.

Career Opportunities: Highlight the various job paths accessible in cybersecurity, such as cybersecurity analyst, ethical hacker, penetration tester, security consultant, incident responder, and others. Emphasize the opportunities for career progression and competitive pay in the field.

Professional Career Development: Highlight the importance of earning industry-recognized cybersecurity certifications and credentials, such as CompTIA Security+, Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and others. These qualifications might improve your credibility and marketability in the job market.

Alumni & Professional Networking: Work with industry partners, cybersecurity groups, and professional associations to provide networking opportunities, internships, mentoring programs, and guest lectures. Collaboration with employers can give students valuable insights into business trends and requirements.

Research-based Education: Develop a dynamic and comprehensive cybersecurity curriculum covering topics such as network security, cryptography, ethical hacking, digital forensics, risk management, and compliance. Use real-world examples, case studies, and interactive exercises to keep students engaged and motivated.

Raising awareness training: Encourage diversity and inclusion in cybersecurity education by actively recruiting members of underrepresented groups, such as women, minorities, and people with various backgrounds. Encourage diversity and provide a helpful learning environment for all students.

By employing these tactics, educational institutions and cybersecurity organizations may effectively attract students to cybersecurity education and train the next generation of cyber experts.

CHAPTER 6

CONCLUSION AND FUTURE WORK

Cybersecurity in education is more than just a technological problem; it is a basic requirement for protecting knowledge and maintaining the integrity of educational institutions. As the digital ecosystem evolves, educational stakeholders must be aware and aggressive in combating cyber dangers. Educational institutions may reduce risks and provide a safe and resilient learning environment for all by investing in strong cybersecurity measures, cultivating a culture of awareness and accountability, and encouraging stakeholder engagement.

Despite the advantages of internet use, such as educational opportunities and enjoyment, this paper emphasizes the significance of cybersecurity awareness in reducing potential threats. It emphasizes the responsibility of schools in promoting critical digital literacy and advising parents on how to supervise their children's online usage.

The paper proposes strategies for increasing cybersecurity education in schools, such as incorporating cybersecurity topics into current curriculum courses, hosting cybersecurity awareness events, and forming cybersecurity organizations or clubs. It promotes active learning methodologies that allow students to tackle cybersecurity challenges individually while receiving advice from educators.

REFERENCES

[1] Adamos, K., et al. "An Analysis of European Union Cybersecurity Higher Education Programs Through the Crowd-Sourced Database CyberHEAD." IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy, vol. 21, no. 5, Sept. 2023, pp. 85–94. EBSCOhost, https://doi.org/10.1109/MSEC.2023.3299348.

[2] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119. https://doi-org.ezproxy.montclair.edu/10.1016/j.cose.2022.102756

[3] AlDaajeh, Saleh, et al. "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education." Computers & Security, vol. 119, Aug. 2022. EBSCOhost, https://doi.org/10.1016/j.cose.2022.102754.

[4] Dawson, Maurice, and Annamaria Szakonyi. "Cybersecurity Education to Create Awareness in Artificial Intelligence Applications for Developers and End Users." Buletin Stiintific, vol. 25, no. 2, July 2020, pp. 85–92. EBSCOhost, https://doi-org.ezproxy.montclair.edu/10.2478/bsaft-2020-0012.

[5] Gasiba, Tiago E., Ulrike Lechner, and Maria Pinto-Albuquerque. "Cybersecurity Challenges in Industry: Measuring the Challenge Solve Time to Inform Future Challenges." Information, vol. 11, no. 11, 2020, pp. 533. ProQuest, http://ezproxy.montclair.edu:2048/login?url=https://www.proquest.com/scholarly-journals/cybersecurity-challenges-industry-measuring/docview/2462539195/se-2, doi:https://doi.org/10.3390/info11110533.

[6] Mughaid, Ala, et al. “An Intelligent Cybersecurity System for Detecting Fake News in Social Media Websites.” Soft Computing - A Fusion of Foundations, Methodologies & Applications, vol. 26, no. 12, June 2022, pp. 5577–91. EBSCOhost, https://doi-org.ezproxy.montclair.edu/10.1007/s00500-022-07080-1.

[7] Shuchi Grover, Brian Broll, and Derek Babb. 2023. Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2023). Association for Computing Machinery, New York, NY, USA, 980–986. https://doi.org/10.1145/3545945.3569750

[8] Faiza Tazi, Sunny Shrestha, and Sanchari Das. 2023. Cybersecurity, Safety, & Privacy Concerns of Student Support Structure for Information and Communication Technologies in Online Education. Proc. ACM Hum.-Comput. Interact. 7, CSCW2, Article 264 (October 2023), 40 pages. https://doi.org/10.1145/3610055

[9] Vandana P. Janeja, Abu Zaher Md Faridee, Aryya Gangopadhyay, Carolyn Seaman, and Amy Everhart. 2018. Enhancing Interest in Cybersecurity Careers: A Peer Mentoring Perspective. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18). Association for Computing Machinery, New York, NY, USA, 384–389. https://doi.org/10.1145/3159450.3159563

[10] Richard Weiss, Casey W. O'Brien, Xenia Mountrouidou, and Jens Mache. 2017. The Passion, Beauty, and Joy of Teaching and Learning Cybersecurity. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17).

Association for Computing Machinery, New York, NY, USA, 673–674. https://doi.org/10.1145/3017680.3017692

[11] Lydia Kraus, Valdemar Švábenský, Martin Horák, Vashek Matyás, Jan Vykopal, and Pavel Celeda. 2023. Want to Raise Cybersecurity Awareness? Start with Future IT Professionals. In Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1 (ITiCSE 2023). Association for Computing Machinery, New York, NY, USA, 236–242. https://doi.org/10.1145/3587102.3588862

[12] Vitaly Ford, Ambareen Siraj, Ada Haynes, and Eric Brown. 2017. Capture the Flag Unplugged: an Offline Cyber Competition. In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17). Association for Computing Machinery, New York, NY, USA, 225–230. https://doi.org/10.1145/3017680.3017783

[13] Ahangama, S. Relating Social Media Diffusion, Education Level and Cybersecurity Protection Mechanisms to E-Participation Initiatives: Insights from a Cross-Country Analysis. Inf Syst Front 25, 1695–1711 (2023). https://doi.org/10.1007/s10796-023-10385-7

[14] Blažič, B.J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. Educ Inf Technol 27, 3011–3036 (2022). https://doi.org/10.1007/s10639-021-10704-y

[15] An, Q., Hong, W.C.H., Xu, X. et al. How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. Int. J. Inf. Secur. 22, 305–317 (2023). https://doi.org/10.1007/s10207-022-00637-z

[16] Venter, Isabella M., et al. "Cyber security education is as essential as “the three R's”." Heliyon 5.12 (2019).

[17] Mika Karjalainen, Samir Puuska, and Tero Kokkonen. 2021. Measuring Learning in a Cyber Security Exercise. In Proceedings of the 12th International Conference on Education Technology and Computers (ICETC '20). Association for Computing Machinery, New York, NY, USA, 205–209. https://doi.org/10.1145/3436756.3437046

[18] Peker, Yesem Kurt, et al. "Raising cybersecurity awareness among college students." Journal of The Colloquium for Information Systems Security Education. Vol. 4. No. 1. 2016.

[19] Rahman, Nor Azura Ab et al. “The Importance of Cybersecurity Education in School.” International Journal of Information and Education Technology 10 (2020): 378-382.

[20] M. Marimuthu. (2016). Pembelian secara online catat kes penipuan paling tinggipada 2015. [Online]. Available: http://www.nccc.org.my

[21] Mayer, A., 2014. Smartphones Becoming Prime Target for Criminal Hackers. CBC News: http://www.cbc.ca/news/technology/smartphones- becoming-prime-target-for-criminal-hackers-1.2561126.

[22] Newzoo, 2017. Top 50 Countries by Smartphone Users and Penetration. Insights: https://newzoo.com/insights/rankings/top-50-countries-by-smartphone- penetration-and-users/.

[23] Businesstech, 2019. News. How old kids are when they receive their first cellphone – South Africa vs the rest of the world: https://busine sstech.co.za/news/mobile/215997/how-old-kids-are-when-they-receive-their-first -cellphone-south-africa-vs-the-rest-of-the-world/.

[24] Pew Research Centre, 2018. Smartphone Ownership on the Rise in Emerging Economies. Global attitudes and trends: http://www.pewg lobal.org/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economie s/.

[25] Porter, G., 2016. How mobile Phones Are Disrupting Teaching and Learning in Africa. The Conversation: https://theconversation.com/h ow-mobile-phones-are-disrupting-teaching-and-learning-in-africa-59549.

APPENDIX

Survey questions

What is your age?

- Less than 18 years
- 18-24 years
- 25-30 years
- 31-40 years
- 41-50 years
- 51-60 years
- 61-70 years
- More than 70 years

What is your gender?

- Female
- Male
- Transgender
- Do not wish to specify

What is the highest level of education you have completed?

- Less than high school
- High school graduate
- Bachelor's degree program
- Masters degree program
- Other. (Please Specify)

Have you taken or taught a course on computer security?

- Yes
- No

How important do you feel cybersecurity or safety is for you?

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important

What is your current occupation?

- Employed
- Unemployed
- Student
- Retired
- Do not wish to specify

Have you ever taken part in cybersecurity awareness campaigns or workshops hosted by your educational institution?

- Yes
- No

How confident are you in your knowledge of understanding basic cybersecurity principles and best practices?

- Extremely confident
- Very confident
- Moderately confident
- Slightly confident
- Not at all confident

Have you ever received formal cybersecurity training or education within the past year?

- Yes
- No

Have you ever worked in the cybersecurity field?

- Yes
- No

How concerned are you about your identity or privacy when using social media?

- Extremely concerned
- Very concerned
- Moderately concerned
- Slightly concerned
- Not at all concerned

Is there anything in specific you wish you had learned in School before your work experience?

Survey Link- https://forms.gle/ipvj4GBtU9tK4hAfA