

Computer Teachers' Perspectives on the Integration of Cybersecurity Concepts into Secondary Computer Curricula in Saudi Arabia

Wejdan Mesfer Alzahrani¹, Majed Gharmallah Alzahrani²

¹Ministry of Education, Jeddah Region, Jeddah, Saudi Arabia

²Department of Curriculum and Instruction, College of Education, University of Jeddah, Jeddah, Saudi Arabia

Correspondence: Majed Gharmallah Alzahrani, Department of Curriculum and Instruction, College of Education, University of Jeddah, Jeddah, Saudi Arabia.

Received: July 12, 2026

Accepted: August 23, 2026

Online Published: September 8, 2026

doi:10.11114/jets.v15i1.9054

URL: <https://doi.org/10.11114/jets.v15i1.9054>

Abstract

Despite research conducted on cybersecurity education at international and regional levels, little empirical data has been collected regarding the Saudi secondary school computer curricula through the perceptions of computer teachers. Hence, this study explores the perspectives of computer teachers in Saudi Arabia towards the inclusion of cybersecurity concepts in computer curricula taught in secondary schools. A cross-sectional design was used with a sample of 414 teachers to collect data through an online questionnaire. Findings show that educators see an average degree of incorporation of cybersecurity issues, and the greatest focus on achieving digital citizenship and digital capabilities of students. On the other hand, the implementation of cybersecurity skills and the evaluation of knowledge among students were viewed as underrepresented in the curriculum. The findings also showed no statistical significance in the difference in the views of teachers, depending on their gender, experience, or enrollment in training courses, indicating that there was a common perspective that was more influenced by the curriculum structure rather than their personal characteristics. The findings illustrate the necessity of curriculum modification that is not confined to the level of conceptual knowledge but incorporates the level of applied, competency-based cybersecurity learning outcomes. The inclusion of real-life exercises, real-life situations, and the form of assessments would help to improve the skills of students to react safely to cyber threats.

Keywords: cybersecurity education, computer curricula, computer teachers' perspectives, Saudi Arabia

1. Introduction

1.1 Background and Context

The modern era is experiencing swift advancements in digital technology, leading to a heightened dependence on computers and the internet across multiple facets of life, particularly within the realm of education (Sandua, 2024). This transformation also resulted in various challenges concerning information security and data protection, thereby rendering cybersecurity concepts indispensable elements even for early levels of education (Al-Fatlawi, 2024). General education is considered a crucial avenue for fostering safe digital awareness among students, thereby enhancing their protection against the growing threats posed by cyber risks (Abbadi, 2025).

The computer curricula show a direct alignment with cybersecurity concepts, as underlying subjects include discussions related to technology, interaction with digital systems, the internet and related networks. The computer teacher possesses an important role in transmitting these concepts to students through either curriculum content or classroom practices. Assessing the extent of incorporating cybersecurity concepts into computer curricula is important, especially from the perspective of computer teachers who teach these courses and develop activities to apply these concepts in practice.

Several modern studies have confirmed the importance of integrating cybersecurity concepts into curricula to increase students' awareness about digital systems and enhance their ability to interact safely with existing technologies. Incorporating cybersecurity as a cross-disciplinary theme can significantly impact learners' readiness by developing awareness and skills to protect their personal data against potential cyber threats (Nadeem, 2024).

A systematic review highlighted the critical need to integrate cybersecurity courses into curricula and consistently

improve these courses to build knowledge about emerging threats (Arishi et al., 2024). To address growing cyber threats, this inclusion in information technology curricula is beneficial both theoretically and practically (Azzeh et al., 2022). From this perspective, cybersecurity education in school is no longer an optional add-on, but is increasingly becoming the core component of fundamental digital literacy, promoting safe technology use, protecting privacy and navigating sensitive interactions in online environments.

1.2 Problem Context in Saudi Arabia

The digitalization of educational institutions is becoming a noticeable trend in Saudi Arabia. As secondary school students are major technology users, the need to enhance their cybersecurity awareness has become critical. Students substantially lack the knowledge regarding the basic concepts of cybersecurity and data protection strategies, making them vulnerable to cyber threats (Mishra et al., 2024). Within online educational environments, the lack of integration of cybersecurity concepts negatively impacts a student's awareness of cybersecurity threats (Nadeem, 2024). A significant proportion of students in technical programs lack the fundamental knowledge and skills to combat cybercrime (Azzeh et al., 2022). Students also find it difficult to differentiate between safe and unsafe online practices, thereby exposing themselves to hacking, blackmail, and online exploitation (Amankwa, 2021). However, providing computer teachers with cybersecurity knowledge can be a helpful approach in improving students' awareness (Serik et al., 2025).

Computer curricula are essential in education, as several educational tools and instructions abundantly rely on the internet to enable searching for information, using digital media for learning, enhancing lesson understanding, undertaking online assessments, and accessing a wide array of educational resources (Ngongpah & Oni, 2025). As Saudi Arabia is moving in the direction of digitalization with a focus on modernization of educational systems and the promotion of safe and responsible use of technology, incorporating cybersecurity concepts is essential for protecting digital space and enhancing the individual capacity to participate safely in the knowledge economy.

1.3 Research Gap

Previous studies have identified the inconsistent integration of cybersecurity concepts into academic programs (Chouki et al., 2020; Nadeem, 2024; Siraj et al., 2015), which highlights the need for empirical research to examine the nature of this integration, especially in the context of the ongoing transformations of educational frameworks in the digital age. Despite research at international and regional levels, little empirical research has been conducted to understand the perspectives of computer teachers regarding the integration of cybersecurity concepts in the Saudi secondary school computer curriculum. Filling this gap is especially important because teachers offer first-hand evidence of how the cybersecurity concepts are reflected in the contents, activities, and evaluation practices.

1.4 Research Questions

This study aimed at addressing the following questions:

- 1) To what degree are cybersecurity concepts integrated into the secondary school computer curricula, as perceived by computer teachers in Saudi Arabia?
- 2) Are there significant differences in computer teachers' perspectives based on gender, years of experience, and number of training courses?

1.5 Research Objectives

The present study aimed at:

- 1) Exploring teachers' perspectives on the extent to which cybersecurity concepts are integrated into secondary school computer curricula in Saudi Arabia.
- 2) Examining potential differences in the perspectives of computer teachers based on gender, years of experience, and number of training courses.

1.6 Significance of the Study

This study is significant, as it addresses a contemporary and innovative issue and contributes to the educational literature in the increasingly expanding field of cybersecurity. This study advances the understanding of data protection, user privacy, and online risk management in the context of Saudi education. Moreover, this study also provides information regarding indicators that educational decision makers and curriculum designers can use to design policies and educational programs to improve cybersecurity awareness among students. The results also contribute significantly to the efforts of national programs to support the goals of Saudi Vision 2030. such as protecting Saudi cyberspace and reinforcing its security. Additionally, this study is vital in training teachers and creating criteria for students to safely use the internet to reduce the impacts of cyber threats.

2. Literature Review

2.1 *Cybersecurity Education in Schools*

In the digital era, where individuals and institutions rely on the internet for several daily activities, protecting electronic systems and data from cyber threats, which could lead to significant financial losses, privacy issues, and adverse impacts on individuals' and institutions' safety is a vital concern (Dawson et al., 2022). According to Dawson et al. (2022), cybersecurity promotes data confidentiality and integrity, continuity of digital services and establishes trust in electronic systems. Cybersecurity ensures data integrity during transmission and processing, provides functionality of digital systems, and reduces interruptions due to cyberattacks while also enabling monitoring of digital activities and data flow in case of data breaches.

Cybersecurity system protects the digital environment from attacks using comprehensive safety measures and strategies. These efforts maintain data confidentiality, prevent unauthorized data access and cyber-attacks while keeping digital infrastructure sustainable and operational (Mountrouidou et al., 2019). Cybersecurity is crucial in protecting individuals' or organizations' informational assets, guaranteeing the business continuity, preserving the confidentiality of stakeholders, and following the laws and regulations concerning information security in addition to establishing trust in digital technologies (Edwards & Weaver, 2024). Cybersecurity not only protects against risks of espionage and online sabotage but also recognize vulnerabilities in computer networks and smart gadgets.

Flexibility, anticipation, and partnership are the hallmarks of cybersecurity. These components are essential technological components, protecting data from technological challenges. Cybersecurity can adapt to new threats and technologies, providing effective solutions against cyber-attack strategies. By incorporating advanced techniques of network monitoring and data analysis, cybersecurity is also proactive in threat detection and mitigation. This approach relies on cooperation, coordination and synergy between security services of institutions and government bodies, and a variety of organizations to exchange information about threats and their solutions. Cybersecurity is defined by continuously updated software, systems, security policies, and protocols. Additionally, cybersecurity highlights the importance of the human element within the security chain and the crucial role played by cybersecurity in reducing human error and counteracting complex social engineering attacks through continuous training and increasing security awareness among users (Diogenes & Ozkaya, 2018).

Achieving cybersecurity requires meeting several basic requirements: highly developed technical skills in operating systems, programming, and networks. Furthermore, academic qualifications and professional licenses are required along with critical thinking and interpersonal communication skills. Additional interlinked strategies include risk assessment, protecting the digital infrastructure, managing identities and access, building security awareness, continuous monitoring and incident response, and system updates and patching to protect against vulnerabilities. These strategies ensure data protection, systems operability, and reduction in cyberattacks (Ciampa, 2012). To remain updated with the latest threats and developments in technologies, the field of cybersecurity requires continuous learning and adherence to existing security policies, standards, and controls, which creates a safe online environment to protect individuals and organizations from cyber-attacks (Triplett, 2023). These findings highlight that cybersecurity is not only an educational topic in schools, but an ethical field that must be constantly taught and updated within school landscapes. For these reasons, early exposure to cybersecurity education is required, as school students are more vulnerable to online risks and still have not developed safe internet use behavior.

2.2 *Integrating Cybersecurity into Computer Curricula*

Cybersecurity education is an essential component in strengthening security in institutions and society. It enhances awareness of cyber-attacks among users. Cybersecurity can improve safe computing behavior, enhance compliance with policies and procedures, and reduce legal and financial cyber vulnerabilities (Vacca, 2017). Since 2011, Saudi Arabia's cybersecurity educational domain significantly expanded, as specialized universities and colleges are established and cybersecurity-related courses are introduced. Such achievements have contributed to the development of national skills to protect online infrastructure (Alghamdi & Younis, 2021). Rahman et al. (2020) and Shoemaker et al. (2023) emphasized the importance of integrating cybersecurity education in computer and general education courses to equip students with the confidence to navigate online space safely, protect their privacy and data, promote responsible online behaviors and tackle digital challenges with greater efficiency. This integration enhances student awareness regarding digital data protection and improves their understanding of emerging cyber threats. Core principles of information technologies (IT) security, such as encryption, authentication, network security, secure design, adversarial thinking, and risk management are incorporated into existing courses instead of introducing them as separate subjects (Mishra et al., 2024). Systematic and cohesive application of these concepts combined with real-life examples and activities can have a greater impact on students' understanding and hands-on skills (Blair, 2017; Siraj et al., 2015). Inadequate cybersecurity education in early education and treating cybersecurity as an elective module leads to severe gaps in graduates'

cybersecurity knowledge. This approach underscores inclusion of cybersecurity as an essential element within programming, database, and software engineering curricula, while also providing supportive educational frameworks for teachers (Siraj et al., 2015). Introducing cybersecurity in computer classes is typically conceptualized as a crosscutting paradigm, and not as an individual isolated unit. This paradigm helps to foster the growth of technical (e.g., protection tactics, threat identification) and non-technical (e.g., digital ethics, responsible citizenship, and safe decision-making over the Internet) competencies.

3. Methodology

3.1 Research Design

This study used a cross-sectional design due to its suitability to address the study objectives. This design allows for systematic data collection from teachers and for comparison across demographic variables.

3.2 Population and Sample

The study population includes computer teachers, both male and female ($n=11,887$), working in the academic year 2024 in intermediate and secondary levels in Saudi Arabia. Simple random sampling was used to collect data from 414 computer teachers. This sample is considered adequate based on statistical power analyses conducting via G*Power software (Faul et al., 2007; Faul et al., 2009), (see Table 1). Simple random sampling improved sample representativeness and increased the findings' generalizability.

3.3 Instrument (Questionnaire)

The questionnaire served as the primary instrument for comprehensive and in-depth data collection regarding trends, views, and perceptions of participants. A questionnaire is a flexible tool to collect data from larger samples. This approach facilitates accurate data collection and statistical analysis. Valid and reliable questionnaires can also be applied in various contexts (Creswell, 2012). The 19 items of the questionnaire were adapted from Alogla and Ali (2022) (items 1-10) and Alhebayib (2022) (items 11-19). All items are answered on a 5 point-Likert scale ranging from 1 (*Strongly disagree*) and 5 (*Strongly agree*).

3.4 Validity and Reliability

3.4.1 Face Validity

The content validity of the questionnaire was assessed by taking suggestions from 10 faculty members specialized in computer education. Face validity was assessed through language accuracy, item clarity, and relevance to stated objectives. The reviewers' feedback was used to modify and improve questionnaire items.

3.4.2 Internal Consistency Validity

The construct validity was tested by computing the Pearson correlation coefficient of a simple random sample of 32 computer teachers (Table 1). This coefficient shows the correlation between answers for each question in the questionnaire, thus indicating highly valid questionnaire items.

Table 1. Correlation coefficients for the questionnaire items

Item	Correlation Coefficient	Item	Correlation Coefficient	Item	Correlation Coefficient
1	.671**	8	.716**	15	.678**
2	.779**	9	.659**	16	.725**
3	.656**	10	.738**	17	.588**
4	.653**	11	.786**	18	.575**
5	.743**	12	.622**	19	.671**
6	.767**	13	.610**	--	--
7	.833**	14	.707**	--	--

** Statistically significant at the level of (.01)

3.4.3 Reliability (Internal Consistency)

Cronbach's alpha was used to assess the internal consistency of the questionnaire. A Cronbach's alpha of .94 indicated acceptable reliability of the questionnaire to measure the perspectives of teachers regarding cybersecurity integration in curricula (George & Mallery, 2024).

3.5 Data Collection Procedure

The questionnaire was designed by Google Forms and sent to the study sample through WhatsApp, and responses were gathered for statistical analysis.

3.6 Data Analysis

For the first research question, means and standard deviations represents the most suitable statistical approach to assess the integration of cybersecurity concepts within secondary school computer curricula (Verma et al., 2024). For the second research question, an independent samples *t*-test and a one-way ANOVA were employed to identify the statistical differences in teachers' perspectives regarding the integration of cybersecurity concepts into computer curricula, based on the variables of gender, years of experience, and the number of training courses in cybersecurity. The level of statistical significance was set at $\alpha \leq 0.05$.

4. Results

4.1 Sample Description

The demographic breakdown of the study sample is shown in Table 2.

Table 2. Description of the study sample

Variable	Variable Categories	Frequency	Percentage
Gender	Male Teacher	186	44.9%
	Female Teacher	228	55.1%
Years of Experience	5 Years and less	94	22.7%
	From 6 to 10 years	134	32.4%
	From 11 to 15 years	90	21.7%
	More than 15 years	96	23.2%
Training Courses	I have never attended these courses.	86	20.8%
	From one course to three courses	230	55.6%
	More than 3 courses	98	23.7%
Total		414	100%

The percentage of female teachers is more than that of their male counterparts. The majority of teachers have 6-10 years of experience, with the lowest proportion of teachers having 11-15 years of experience. This difference demonstrates diverse teaching experiences, allowing for different perspectives regarding computer curricula. Around 80% of teachers have participated in training programs, which indicate that the majority of computer teachers are highly trained. Comparatively, around 20% of computer teachers have not attended any training programs, which may affect their evaluation of cybersecurity concepts in computer curricula. A good demographic balance is evidenced by the sample distribution, which ensures the sample representativeness and increases the generalizability of the findings to the larger population. This demographic distribution represents a wide spectrum of professional backgrounds and training exposure, which increases the validity of the teachers' perspectives presented in the subsequent analysis.

4.2 Level of Cybersecurity in the Curriculum

To answer the first research question, the standard deviations and the means were used to prioritize the questionnaire items that measured the level of cybersecurity integration in the computer curriculum among secondary schools. These were arranged as items in descending order based on mean values in Table 3.

Table 3. Computer teachers' perspective of the degree of inclusion the cybersecurity concepts in secondary computer curricula

Item Number	Item	Mean	Standard Deviation	Level of Agreement	Rank
13	The curriculum includes topics to promote digital citizenship among students.	3.81	.82	Agree	1
17	The curriculum fosters the development of students' digital competencies, equipping them to safeguard themselves and others in the online environment.	3.62	.79	Agree	2
2	The curriculum encompasses the essential concepts of cybersecurity.	3.93	.76	Neutral	3
8	The curriculum delineates techniques for the identifying malware.	3.53	.78	Neutral	4
9	The curriculum encompasses subjects that elucidate the ethical dimensions of cybersecurity.	3.32	.81	Neutral	5
10	The curriculum encompasses subjects that elucidate the legal dimensions of cybersecurity.	3.28	.83	Neutral	6
11	The curriculum offers educational scenarios designed to enhance problem-solving abilities in the realm of cybersecurity.	3.25	.84	Neutral	7
16	The curriculum offers students the chance to engage in discussions related to cybersecurity.	3.21	.93	Neutral	8
18	The curriculum encompasses discussions on the significance of implementing programs aimed at safeguarding personal data.	3.12	.89	Neutral	9
6	The curriculum encompasses subjects that underscore the significance of safeguarding information.	3.10	.74	Neutral	10
4	The curriculum encompasses a diverse array of activities within the realm of cybersecurity.	3.05	.94	Neutral	11
7	The curriculum encompasses a range of illustrative instances of electronic fraud techniques.	3.01	.68	Neutral	12
15	The curriculum encompasses instances of cybersecurity breaches.	2.82	.87	Neutral	13
19	The curriculum encompasses the process of downloading antivirus software on mobile devices.	2.78	.86	Neutral	14
12	The curriculum evolves in tandem with advancements in cybersecurity, reflecting contemporary technological trends.	2.75	.79	Neutral	15
14	The curriculum fosters an understanding of cybersecurity culture.	2.70	.77	Neutral	16
3	The curriculum encompasses a variety of resources designed to impart knowledge of cybersecurity principles.	2.68	.84	Neutral	17
1	The curriculum encompasses specialized lessons that address various aspects of cybersecurity.	2.65	.82	Neutral	18
5	The curriculum includes assessment methods that measure the extent of students' understanding of cybersecurity concepts.	2.62	.81	Neutral	19
Overall Mean		3.08	.81	Neutral	

Table 3 provides an answer to the first research question. According to the findings, there was a neutral position; the mean results were (3.08) with a standard deviation of (.81). The scores of the items averaged between 2.62 and 3.81, and the standard deviations were between .68 and .94. The item that reported the highest mean score was item number 13, which states that the curriculum incorporates the topics to encourage students into becoming good digital citizens. The average score of this item was 3.81, with a standard deviation of .82, which indicates that there was an agreement between the respondents on this item. The second item was item number 17 that claims that the curriculum encourages the growth of digital skills in students, enabling them to protect themselves and other individuals in the online space. The mean score of this item was 3.62 with a standard deviation of .79 showing an agreement between teachers.

Conversely, the lowest mean score was item number 5, which is: The curriculum has assessment approaches that evaluate the level of student knowledge of cybersecurity concepts. The average score of this item was 2.62 with a standard deviation of .81, which is a neutral response. In the same way, the least ranked items were located in areas of assessment and practical implementation, but not in general awareness. The results indicate that there was a neutral effect of incorporating the concept of cybersecurity into the computer curriculum in secondary schools. This result implies that cybersecurity is taught within the curriculum based on the level of awareness and conceptual learning, but not on applied learning, systematic assessment, and skill-based learning. The importance of digital literacy and responsible online behavior has been highlighted, but the practical and assessment areas do not appear to be properly addressed.

This paper explains the obtained findings by the design of the curriculum, which seems to be insufficient in terms of focusing on the acquisition of practical skills and the delivery of evaluation instruments that can adequately track the level of student understanding of the concepts of cybersecurity. This deficit can be attributed to the fact that there is inadequate specialized training of teachers and inadequate clear strategies of continuous curriculum development, which should be aligned with rapidly evolving digital threats.

The results were consistent with the study by Nadeem (2024), which reported a desire among the students to study cybersecurity content when it was a part of the curriculum. Nevertheless, the coordination between experts and teachers

turned out to be a difficult issue, alongside the issue of continuing to apply this content. This result illustrates the limited practical integration in the curriculum of the secondary school. This research is an exception to the results of Azzeh et al. (2022), who showed that the experimental application of cybersecurity into the curriculum led to a significant improvement in knowledge among students. The current results, however, did not imply improvement, which could be explained by the absence of implementation.

4.3 Differences by Gender

To answer the second research question, an independent samples *t*-test was conducted to measure the potential difference of male and female computer teachers regarding the level of the integration of cybersecurity concepts in computer curricula in secondary schools. Table 4 illustrates the comparison of teacher views by gender.

Table 4. Comparison of computer teachers' perspective based on gender

	Gender	Mean	Standard Deviation	<i>t</i> -value	<i>p</i> -value
The level of incorporating cybersecurity concepts into computer curricula	Male	3.41	.65	.439	.661
	Female	3.52	.83		

According to Table 4, the independent samples *t*-test revealed a *p*-value greater than .05. These results reveal no statistically significant differences in the mean perspective of teachers on the inclusion of concepts of cybersecurity in the curriculum of secondary schools according to gender. The results of this analysis show a congruence of views between male and female educators regardless of gender, which indicates that the issue of cybersecurity is regarded as a common priority among all educational workers. This observation shows that male and female teachers have similar assessments regarding cybersecurity integration.

4.4 Differences by Years of Experience

A one-way ANOVA was employed in order to determine whether there was a statistically significant difference in the views of teachers about the degree of inclusion of cybersecurity concepts in secondary school computer curricula according to years of experience. Table 5 exhibits the results of this analysis.

Table 5. Comparison of computer teachers' perspective based on years of experience

	Source of Variation (SV)	Sum of Squares (SS)	Degrees of Freedom (DF)	Mean Squares (MS)	<i>F</i> -Ratio (<i>F</i>)	<i>p</i> -value / Prob > <i>F</i>
The level of incorporating cybersecurity concepts into computer curricula	Between groups	1.528	3	.764	.439	.321
	Within groups	166.57	226	.669		
	Total	168.098	229	.716		

According to Table 5, the *p*-value is greater than .05, which illustrates that there are no significant differences based on years of experience. This finding is supported by various explanations. First, the knowledge of computer instructors appears to be relatively homogeneous, which creates insignificant differences in their outlooks on the implementation of the principles of cybersecurity, regardless of their professional experience. Second, the study of cybersecurity diseases can be poorly implemented in the educational programs where all educators can be seen as having the same view, regardless of their qualifications. This result supports previous studies since the awareness of teachers on cybersecurity topics, according to the study by Azzeh et al. (2022), has a lower connection with years of experience and more with the overall culture of ubiquity created by rapid digital changes and the increasing reliance on technology in education. The experiment conducted by Alshwarh (2024) proved experimentally that years of experience did not affect the cybersecurity knowledge of teachers in schools within the Hashemite Kingdom of Jordan. Nadeem (2024) illustrated that challenges of integrating cybersecurity concepts are largely explained by organizational and institutional factors, and not by an individual, which clarifies the absence of differences associated with professional experience. This tendency was supported by the study of Serik et al. (2025), which showed that the need to work on the curriculum and implement the concept of cybersecurity is a common requirement on the part of educators, regardless of their years of experience. Accordingly, the fact that no statistically significant differences were found implies that the perceived level of cybersecurity integration is an experience that teachers go through, irrespective of tenure.

4.5 Training Courses Differences.

A one-way ANOVA was conducted to determine if there were statistically significant differences on the perspectives of computer teachers on how much the concept of cybersecurity has been integrated into secondary school computer curriculum based on the number of training courses taken on computer security. Table 6 shows the results of this analysis.

Table 6. Comparison of computer teachers' perspective based on the number of training courses in the field of cybersecurity

	Source of Variation (SV)	Sum of Squares (SS)	Degrees of Freedom (DF)	Mean Squares (MS)	F-Ratio (F)	p-value / Prob > F
The level of incorporating cybersecurity concepts into computer curricula	Between groups	1.354	3	0.451	1.564	0.199
	Within groups	65.185	226	0.288		
	Total	66.539	229	0.369		

According to Table 6, the p -value of the one-way ANOVA is more than .05, which contributes to the assumption that statistically significant differences in the average perspective of teachers regarding the extent of cybersecurity concepts taught in secondary school computer curricula do not exist, as it is associated with the number of training courses in cybersecurity. The study explains this finding by the fact that there are high chances that the available cybersecurity training programs are either ineffective or that the courses that the teachers were taking were insufficient to induce a significant change in their responses. This result implies that even attending training classes might not be enough to fully increase the understanding of cybersecurity concepts among instructors; rather, more specialized training programs may need to be required.

This finding corresponds to the results of other studies. As illustrated by Nadeem (2024), the challenges in the implementation of cybersecurity concepts are not directly related to the number of training courses offered to teachers, but rather depend on institutional policies and the quality of learning programs. This trend was supported by Azzeh et al. (2022), who found that the knowledge of cybersecurity among teachers has become a dominant requirement based on the necessities of technological transformation, regardless of their participation in the specialized training program. Additionally, Serik et al. (2025) showed that the assimilation of cybersecurity concepts has become a common need of all teachers, regardless of their level of training, meaning that awareness of such concepts has become a part of the educative culture, regardless of the amount of training they have undergone. Consequently, the findings indicate that perceived integration of cybersecurity concepts is influenced more by the structure and implementation conditions of the curriculum than by the demographics of individual teachers and the possibility of being exposed to training.

5. Discussion

5.1 Interpretation of the Main Finding

The objective of this study was to determine the opinion of computer teachers regarding the extent to which cybersecurity concepts are applied to the computer curriculum in secondary schools in Saudi Arabia. The results showed that the views of teachers indicated a moderate degree of incorporation of the concept of cybersecurity into computer curricula, and the mean score was 3.08. This observation suggests that cybersecurity education is included in the curriculum, but the practice of cybersecurity remains limited in terms of content, application and systematic implementation.

The ranking of questionnaire items gives a better idea of how cybersecurity is reflected in the curriculum. The item that was rated as highest was associated with advancing digital citizenship to students, with a mean score of 3.81. This finding shows that the content of the curriculum places more emphasis on values, awareness, and responsible online behaviors. On the same note, participants conceded that the curriculum promotes digital skills in students and their capacity to defend themselves and other users in the virtual world.

Conversely, the least-ranked items were related to assessment and practical application, specifically the declaration that the curriculum comprises methods of assessment, which gauge the knowledge of students regarding cybersecurity concepts. This result means that the concept of cybersecurity integration is more apparent than the applied and task level, realistic situations, quantifiable skills, and assessment instruments. In line with this finding, the results also indicate that cybersecurity as a field is brought in more as a form of awareness as opposed to an instructional field that involves skills, and this approach could hinder the capacity of students to transfer theoretical knowledge to practical, safe online behaviors.

5.2 Comparison with Previous Studies

The results of this research are aligned with numerous research studies that have been conducted previously and reveal inconsistency and a lack of integration of cybersecurity in educational programs (Nadeem, 2024; Siraj et al., 2015). Specifically, the level of neutrality indicated by teachers is consistent with the systematic review of Arishi et al. (2024), who underlined that cybersecurity education needs to be constantly updated and supported in the field to be up to date with the changes in threats. The results are also consistent with the findings by Nadeem (2024), who found that the incorporation of cybersecurity into computer curricula will result in greater engagement and awareness of learners, and the inclusion of real-world applications and practical exercises makes it happen. Nonetheless, Nadeem (2024) also pointed out problems with collaboration between specialists and teachers and the inability to maintain integration unless

it is supported by the institution. This result can be used as a pertinent clarification as to why the present research has found that cybersecurity integration has been reflected in general curriculum topics (like citizenship) and is only weak in applied practices and assessment models. In contrast, the results are inconsistent with Azzeh et al. (2022), who found that the experimental approach of integrating the concepts of cybersecurity into the curriculum led to a significant enhancement in cybersecurity knowledge among students. This finding is a deviation that can be explained by methodological and contextual differences. Azzeh et al. (2022) used a quasi-experimental pre-and post-test study design, and the integration was structured teaching interventions. Conversely, this study determined the level of cybersecurity integration as perceived by teachers in an established curriculum framework. Thus, the difference can be explained by the fact that experimental implementation generates more powerful learning outcomes compared with normal curriculum incorporation, which are not backed up by organized practical activities and assessment systems. Serik et al. (2025) also confirmed the current study results by stating that cybersecurity integration requires teacher readiness, curriculum implementation, and real-world training opportunities to be effective.

5.3 No Differences Between Variables

The findings showed that the difference in participant views did not statistically differ regarding gender, years of experience, or the number of training courses taken. This result suggests that teachers have a consistent vision of cybersecurity integration irrespective of their demographic traits and work experience. This observation can be explained by institutional and curriculum-based aspects of teaching. The introduction of the concepts of cybersecurity depends much on the content of the curriculum, the organization of the learning process, and the presence of assessment tools. By extension, when the curriculum in question offers limited applied cybersecurity activities and does not specifically offer methods of assessment, teachers will have similar views in various groups due to their reaction to the same instructional content and constraints.

Moreover, the findings indicate that cybersecurity awareness has turned into a culture of education affected by fast-paced digital transformation and is not predetermined by the personal features of teachers. This finding is aligned with Azzeh et al. (2022), who showed that digital requirements are more important in making individuals more aware of cybersecurity issues than demographic factors. This finding also aligns with Serik et al. (2025), who emphasized that cybersecurity integration is a requirement among teachers, irrespective of the years of service.

In terms of training courses, the lack of significant differences may indicate that the level of involvement in training programs cannot be unambiguously related to an increased perspective of cybersecurity integration in training programs. This null finding could perhaps trigger the fact that training courses are not closely tied to curriculum implementation, or they must not be structured to equip teachers with practical instructional strategies and assessment methods, which would help them identify a more intensive curriculum implementation. Nadeem (2024) provides support for this explanation, who asserted that institutional policies and the quality of educational programs tend to dominate the issues of integration instead of individual involvement in training.

Last, this study substantiates the importance of more comprehensive incorporation regarding cybersecurity into computer curricula, developing learning materials that are cognizant of technological advances, and training the computer educator to be able to effectively apply the concept of cybersecurity in classroom instruction. This type of curriculum development corresponds to the national priorities of Saudi Arabia, such as enhancing digital protection, securing cyberspace, and aiding the educational process in accordance with technological progress.

6. Conclusion

This research was focused on examining the perspective of teachers regarding which the concepts of cybersecurity are being taught in computer programs in Saudi Arabia, and if there are any differences according to gender, years of experience, and number of training courses. The results showed that computer teachers' perspectives were relatively neutral regarding the incorporation of cybersecurity concepts in computer curricula. Despite this finding, it is important to recognize that the knowledge about cybersecurity is only elementary and limited in scope in the secondary school computer curriculum, with no activities and evaluation methods used to support this knowledge.

The findings also showed that the alignment with curricula was highest when related to the issues of digital citizenship and students' digital competencies. These results suggest that there is an increased emphasis on electronic awareness and responsible use of electronic media. In contrast to this finding, the lowest scores were associated with evaluation and applied cybersecurity practices, which included assessment of student knowledge of cybersecurity concepts and improving practices. The finding demonstrated imbalanced curriculum development, with cybersecurity considered not as a well-defined curriculum cluster of measurable skills, but rather a space for concept and awareness building. Additionally, the lack of difference in demographic and training variables means that teachers have similar perspectives regarding the integration of cybersecurity, as they are implementing the same cybersecurity curriculum framework and face the same limitations related to teaching, regardless of their sub-types of teaching profession.

6.1 Implications of Practical Significance to Curriculum Designers and Teachers

This research has a number of implications for curriculum developers, educators in charge in Saudi Arabia, and computer teachers. First, the neutral stage of incorporation shows that the notion of cybersecurity is partially represented in the curriculum, especially when it comes to digital citizenship, awareness, and overall internet safety. Nevertheless, the lack of focus on applied learning and assessment shows the necessity of developing curricula that are beyond awareness of competence-based learning outcomes. Second, the results indicate that reform in curriculum must focus on the introduction of practical cybersecurity exercises, including simulated exercises, problem-solving, exercises on secure behavior, and structured classroom discussion with real examples of cyber threats. These additions would enhance the skills of students to identify and react to risks instead of gaining knowledge about cybersecurity through abstract concepts. Third, the placement of assessment-related items implies that curriculum revision must take into consideration measurable indicators and evaluation techniques that determine the knowledge and skills of students in cybersecurity. These techniques involve the development of classroom-based assessment tools, rubrics, practical assignments, and an online project that assesses safe online behavior, password security, malware identification, and data protection behavior. Fourth, teacher support should be enhanced by the creation of an operational guide (teacher guide) or a training kit that offers classroom activities, teaching approaches, and examples. It is also important to arrange training workshops on how these resources can be effectively used by teachers. This approach is even more essential since teachers are the most important source through which the concepts of cybersecurity are translated and manipulated in the curriculum material to real-life student learning experiences.

6.2 Educational and Policy Implications

The implications of the present research are of great importance for Saudi Arabia curriculum developers, policymakers in education, and computer educators. The neutral findings regarding cybersecurity integration reveals that cybersecurity topics have been incorporated into the present layouts of computer curricula, but these topics must be deepened sufficiently to ensure that students learn meaningful and measurable skills. As such, the task of curriculum reform should be to focus on competency-based cybersecurity learning outcomes instead of confining cybersecurity education to the concept of general awareness and citizenship.

Besides, the findings also highlight the necessity to incorporate cybersecurity concepts more comprehensively into the computer programs by enhancing applied learning. It involves the integration of realistic education situations, realistic practice, and problem-solving tasks that mirror real cyber threats that include malware, phishing, electronic fraud, and personal data breaches. This sort of practical integration is necessary to turn cybersecurity into abstract knowledge into practical digital behavior and protective decision-making by the students in the secondary school.

The results also reveal the need to enhance the assessment practices in computer curricula. The poor position of the assessment-related items indicates that curriculum developers need to incorporate the assessment instruments that can be used to assess the cybersecurity knowledge and competencies of students. These can be classroom-based tests, online projects, practical, and structured rubrics wherein their competency in implementing cybersecurity concepts within real-life online settings is tested.

In addition, the research contributes to the necessity of providing computer educators with learning materials that would support the successful delivery of cybersecurity material. It is highly suggested that an operational guide (teacher guide) should be developed, or a training package containing classroom tasks, instructional situations, and examples of use should be created. It is also necessary to organize training workshops on the effective use of these resources among teachers, especially since they are the main medium through which the cybersecurity concepts will reach the students. Last, national priorities can be integrated into the study findings as it assists in efforts geared toward protecting cyberspace and enhancing digital security. Making cybersecurity a part of school curricula should help to create a generation of digitally responsible individuals, sustain protective use of educational technologies, and enhance the digital protection capacity of the country in line with the Saudi educational transformation.

6.3 Limitations

Although the findings are important, the study has limitations, which must be noted. First, the research was based on the opinions of teachers distributed by the questionnaire, which does not imply analysis of the curriculum content but the perceived integration of the curriculum. As a result, the answers of teachers are likely to be affected by their understanding of the content of the curriculum, teaching, and their exposure to cybersecurity ideas. Second, the research was targeted at computer teachers in Saudi Arabia during the 2024 academic year. Although the sample size was large and representative, the results may not reflect the current context and period of education. Thus, care should be used with the study findings to avoid making generalizations about other levels of education or in other countries.

6.4 Future Research Directions

According to the results, future studies are needed to better understand the issues of cybersecurity integration in schools. The next study could carry out an extensive survey of computer learning curriculum at the secondary level in order to determine how cybersecurity concepts are integrated and how it is up-to-date with current technological trends. Moreover, future studies could examine how the application of modern pedagogical models in the computer curriculum, i.e., project-based or problem-based learning, influences the development of the concept of cybersecurity among secondary school students. Furthermore, the study can be expanded in the future by utilizing mixed-method strategies to integrate cybersecurity into the curriculum by using questionnaires to the teachers and curricula content analysis, observation in the classroom, and student performance measurements. These methods would give a more detailed picture of the way cybersecurity concepts are taught, practiced, and assessed in actual school settings.

Acknowledgments

The authors acknowledge the faculty members who have assessed the instrument and the teachers who have participated in this study.

Author contributions

All authors contributed equally to the study, including the study design, data collection, data analysis, interpretation of the findings and preparation and revision of the manuscript. All authors read and approved the final manuscript.

Funding

Not applicable.

Competing interests

The authors declare no competing interest.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Redfame Publishing.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

References

- Abbad, D. (2025). Digital gaps and cyber risks: Strategies to ensure equal opportunities and digital education security. *International Journal of Information & Digital Security*, 3(2), 19–32. <https://doi.org/10.54878/ba2nbk39>
- Al-Fatlawi, H. H. (2024). Awareness of cyber security aspects in distance education. *Journal of Pedagogical Sociology and Psychology*, 6(1), 77–88. <https://doi.org/10.33902/jpsp.202424403>
- Alghamdi, M. Y., & Younis, Y. A. (2021). The use of computer games for teaching and learning cybersecurity in higher education institutions. *Journal of Engineering Research*, 9(3), 143–152. <https://doi.org/10.36909/jer.v9i3A.10943>
- Alhebayib, M. A. (2022). The degree of cybersecurity awareness among male and female graduate students at the College of Education at Imam Muhammad bin Saud Islamic University and ways to enhance it from their point of view. *Journal of Education Studies- Imam Muhammad ibn Saud Islamic University*, 1(30), 273-326.

<https://journals.imamu.edu.sa/index.php/joes/article/view/2085>

- Alogla, R. A., & Ali, N. A. (2022). The degree of awareness of the concepts of cybersecurity among computer male and female teachers in Hail city. *Journal of Arab Studies in Education & Psychology*, 144(2), 277-300. <https://doi.org/10.21608/saep.2022.263396>
- Alshwarh, K. S. S. (2024). The degree of teachers' awareness of cybersecurity: A field study according to Jordanian school teachers' perspective. *Journal of the Association of Arab Universities for Higher Education Research*, 44(2), 415–436. <https://doi.org/10.36024/1248-044-002-024>
- Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. *Journal of Information Security*, 12(4), 233-249. <https://doi.org/10.4236/jis.2021.124013>
- Arishi, A. A., Kamarudin, N. H., Abu Bakar, K. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications*, 15(12), 467–478. <https://doi.org/10.14569/IJACSA.2024.0151249>
- Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). *Adopting the cybersecurity concepts into curriculum: The potential effects on students' cybersecurity knowledge* [Preprint]. arXiv. <https://doi.org/10.11591/ijeecs.v25.i3.pp1749-1758>
- Blair, T. (2017). *Investigating the cybersecurity skills gap*. (Publication No. 10623377) [A Capstone Project, Utica College]. ProQuest Dissertations & Theses.
- Chouki, M., Talea, M., Okar, C., & Chroqui, R. (2020). Barriers to information technology adoption within small and medium enterprises: A systematic literature review. *International Journal of Innovation and Technology Management*, 17(01), 2050007. <https://doi.org/10.1142/S0219877020500078>
- Ciampa, M. (2012). *Security+ guide to network security fundamentals* (4th ed.). Course Technology, Cengage Learning.
- Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Pearson.
- Dawson, K., Antonenko, P., Xu, Z., Wusylko, C., & Koh, D. (2022). Promoting interdisciplinary integration of cybersecurity knowledge, skills and career awareness in preservice teacher education. *Journal of Technology and Teacher Education*, 30(2), 275-287. <https://doi.org/10.70725/240208fzioim>
- Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics*. Packt Publishing.
- Edwards, J., & Weaver, G. (2024). *The cybersecurity guide to governance, risk, and compliance*. John Wiley & Sons. <https://doi.org/10.1002/9781394250226>
- Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, 41, 1149-1160. <https://doi.org/10.3758/BRM.41.4.1149>
- Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, 39, 175-191. <https://doi.org/10.3758/BF03193146>
- George, D., & Mallery, P. (2024). *IBM SPSS statistics 29 step by step: A simple guide and reference* (18th ed.). Routledge. <https://doi.org/10.4324/9781032622156>
- Mishra, S., Draus, P., Slonka, K., & Bromall, N. (2024). What do high school students know about the field of cyber security? A survey of perception and experiences. *Issues in Information Systems*, 25(3), 36–46. https://doi.org/10.48009/3_iis_2024_104
- Mountroidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. In *ITiCSE-WGR '19: Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education* (pp. 157–176). Association for Computing Machinery. <https://doi.org/10.1145/3344429.3372507>
- Nadeem, A. (2024). Cybersecurity as a crosscutting concept across an undergrad computer science curriculum: An experience report. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education* (Vol. 1, pp. 916–922). Association for Computing Machinery. <https://doi.org/10.1145/3626252.3630821>
- Ngongpah, G., & Oni, O. Y. (2025). Exploring the impact of digital technologies in education: A comprehensive review. *Asian Journal of Education and Social Studies*, 51(6), 1254–1264. <https://doi.org/10.9734/ajess/2025/v51i62071>

- Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5), 378–382. <https://doi.org/10.18178/ijiet.2020.10.5.1393>
- Sandua, D. (2024). *The double sides of technology: Internet addiction and its impact on today's society*.
- Serik, M., Tleumagambetova, D., Tutkyshbayeva, S., & Zakirova, A. (2025). Integration of cybersecurity into computer science teachers' training: A systematic review. *International Journal of Engineering Pedagogy*, 15(4), 57–75. <https://doi.org/10.3991/ijep.v15i4.53127>
- Shoemaker, D., Sigler, K., & Shoemaker, T. (2023). *Teaching cybersecurity: A handbook for teaching the cybersecurity body of knowledge in a conventional classroom*. CRC Press. <https://doi.org/10.1201/9781003187172>
- Siraj, A., Taylor, B., Kaza, S., & Ghafoor, S. (2015). Integrating security in the computer science curriculum. *ACM Inroads*, 6(2), 77–81. <https://doi.org/10.1145/2766457>
- Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, 3(1), 47–67. <https://doi.org/10.53889/ijses.v3i1.132>
- Vacca, J. R. (Ed.). (2017). *Computer and information security handbook* (3rd ed.). Morgan Kaufmann.
- Verma, R., Verma, S., & Abhishek, K. (2024). *Research methodology*. Booksclinic Publishing.