EXCELLENCIA
INTERNATIONAL MULTI-DISCIPLINARY JOURNAL OF EDUCATION
Volume 03, Issue 2, 2025 ISSN (E): 2994-9521

Criteria and Levels for Assessing Students' Cybersecurity Culture through Digital Platforms

Hojiakbar Zafarjon-ogli Muhammadjonov
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Lecturer of the Department of Digital Technologies and Information Security

Abstract

The study explores the assessment criteria and levels of students' cybersecurity culture through digital platforms, emphasizing the growing significance of cybersecurity awareness in educational settings. It highlights the role of individual engagement, organizational norms, and curriculum integration in fostering a robust cybersecurity culture. The literature review examines security behaviors, the impact of digital citizenship, and tailored cybersecurity education strategies, including game-based learning and awareness frameworks. The findings underscore the need for a multi-faceted approach to enhancing cybersecurity culture, ensuring students are well-equipped to navigate an increasingly complex digital environment.

Keywords: *Cybersecurity Awareness; Digital Platforms; Security Culture; Educational Strategies; Cybersecurity Education*

Introduction

The exploration of students' cybersecurity culture through digital platforms has gained significant attention in recent years, reflecting the increasing importance of cybersecurity awareness in an ever-evolving digital landscape. The literature reveals a multifaceted approach to understanding and enhancing cybersecurity practices among individuals, particularly students, who are positioned as future decision-makers in combating cyber threats.

[1] emphasizes the critical role of individual users in cybersecurity, arguing that while many perceive security as the sole responsibility of specialists, it is essential for individuals to actively engage in security practices. This study highlights a concerning gap in security awareness and engagement among individuals in Southern California, suggesting that despite numerous awareness campaigns, many users remain uninformed about effective security measures. This foundational understanding sets the stage for subsequent discussions on the broader implications of security culture within organizations.

Building on this concept, [2] introduce the notion of security culture as a framework for understanding everyday cybersecurity behaviors. They identify positive and negative security behaviors and stress the significance of organizational norms and values in shaping security practices. Their findings underscore the complexity of security culture, noting the existence of subcultures within organizations that may exhibit conflicting values. This nuanced perspective is crucial for developing effective cybersecurity strategies that resonate with diverse organizational environments.

[3] further expand the discourse by examining the interplay of trust and ethical conduct within organizations. They argue that fostering a cybersecurity culture requires establishing a network of champions who advocate for security awareness and act as points of contact within organizations. This collaborative approach underscores the need for a collective effort in promoting cybersecurity practices and highlights the importance of ethical behavior in decision-making processes related to security.

The focus shifts to the educational context in [4], who investigate the level of awareness and knowledge regarding digital citizenship practices among students and faculty in distance learning environments. Their findings reveal significant gaps in knowledge, particularly concerning digital law and safety, suggesting that both students and educators require enhanced training in digital citizenship to navigate the complexities of the digital world effectively.

In the context of high school education, [5] propose a cybersecurity threat awareness framework tailored for students in Qatar. Their research identifies various successful approaches to delivering cybersecurity awareness, including conventional methods, educational videos, and game-based learning. This study highlights the importance of engaging students through diverse educational strategies to foster a robust understanding of cybersecurity threats.

[6] contribute to the discussion by emphasizing the necessity of cybersecurity awareness not only for cybersecurity personnel but also for operational managers. Their findings suggest that comprehensive training is essential for employees to tackle cybersecurity threats, particularly in remote work environments. The study also points to significant variations in cybersecurity awareness and behavior across different countries, indicating the need for tailored awareness programs.

Lastly, [7] address the integration of cybersecurity concepts into academic curricula, highlighting the critical role universities play in enhancing students' cybersecurity knowledge. Their pilot study reveals a concerning lack of awareness among students regarding cybersecurity risks and protective measures. The authors propose a structured methodology for incorporating cybersecurity topics into non-security courses, aiming to bridge the knowledge gap and promote a culture of security awareness among students.

Together, these articles provide a comprehensive overview of the current landscape of cybersecurity culture, awareness, and education, illustrating the multifaceted challenges and opportunities that exist in fostering a secure digital environment for students.

2. Literature review

In the article "SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD," [1] delves into the critical role that individual users play in maintaining cybersecurity. The article emphasizes that while cybersecurity specialists are essential for protecting systems and networks, the responsibility also lies with the everyday user. This perspective is crucial, as it challenges the prevailing notion that cybersecurity is solely a technical issue managed by professionals.

The study focuses on assessing the current level of security awareness and engagement among individuals in Southern California, particularly in Los Angeles County and the Inland Empire. The findings reveal a concerning lack of awareness and proactive engagement in cybersecurity practices among the general public. This gap in knowledge and action underscores the importance of cybersecurity-awareness campaigns, which aim to foster secure online behaviors among users. The article highlights that these campaigns are not merely informative; they are essential for cultivating a culture of security that encourages individuals to take ownership of their online safety.

The article's critical evaluation of individual engagement in cybersecurity practices is particularly relevant in today's increasingly digital world. [1] identifies that many users feel intimidated by the complexities of cybersecurity, often adopting a passive attitude towards their online safety. This mentality can lead to significant vulnerabilities, as users may neglect basic security measures that could protect them from cyber threats. The study calls for a shift in this mindset, advocating for a more proactive approach where individuals recognize their role in cybersecurity.

Furthermore, [1] proposes that understanding the current level of security awareness can inform the development of more effective awareness campaigns. By identifying specific areas where users lack knowledge, campaigns can be tailored to address these gaps, thereby enhancing the overall cybersecurity culture. This targeted approach is essential for increasing user engagement and fostering a sense of responsibility among individuals regarding their online security.

The article "Cyber Security Behaviour In Organisations" by [2] provides a comprehensive examination of the complexities surrounding the concept of security culture within organizations. The authors argue that security culture is inherently contested, highlighting the absence of a universally accepted definition or composition. This ambiguity presents challenges for organizations seeking to cultivate an effective cybersecurity culture among their members.

[2] delineate the dual nature of security behaviors, categorizing them as either positive or negative. Positive security behaviors are characterized by actions that enhance daily freedoms while maintaining security, whereas negative security behaviors focus on eliminating threats. This distinction is crucial as it underscores the need for a balanced approach to cybersecurity that does not infringe upon individual liberties while still ensuring organizational safety.

The concept of security culture is further explored through the lens of shared norms and values that shape the mindsets of organizational members. The authors emphasize that these shared beliefs are pivotal in forming a cohesive security culture, which in turn influences the overall security posture of the organization. The presence of subcultures within larger organizations can complicate this dynamic, as conflicting values may emerge, leading to challenges in establishing a unified approach to cybersecurity.

Moreover, the article discusses the impact of various factors on the development of security culture, including cultural norms and the level of trust in organizational protective measures. The authors suggest that these elements can significantly affect how individuals perceive and engage with security practices. A strong security culture, as posited by [2], is essential for mitigating human-related security breaches, which are often the result of inadequate security awareness or conflicting attitudes toward security protocols.

The article "Developing a cyber security culture: Current practices and future needs" by [3] provides a comprehensive examination of the essential components necessary for cultivating a robust cybersecurity culture within organizations. The authors emphasize the significance of mutual trust

between employees and the organization, highlighting that such trust is foundational for effective security practices. This trust is not merely a byproduct of good relationships; it is a critical element that influences how security activities are perceived and executed within an organization.

The article also delves into the ethical dimensions of cybersecurity culture, positing that behavior and decision-making should adhere to a moral code that defines right and wrong. This ethical framework is crucial for fostering an environment where security is prioritized and integrated into daily operations. The authors argue that establishing clear ethical guidelines can help shape employees' attitudes towards cybersecurity, ultimately leading to more responsible behavior regarding security practices.

Another key insight from the article is the concept of "champions" within organizations. Champions are individuals who actively promote cybersecurity awareness and serve as points of contact for security-related queries and initiatives. The presence of these champions is critical in driving engagement and enhancing the overall security culture, as they can influence their peers and help disseminate important security information effectively.

[3] also draw on the work of AlHogail (2015a, 2015b) and Alnatheer (2015) to support their arguments regarding the necessity of a structured approach to developing and assessing cybersecurity culture. They propose that organizations should adopt frameworks that not only cultivate a security-oriented mindset but also allow for the measurement of cultural maturity in terms of cybersecurity practices.

The article titled "Comparative analysis of students and faculty level of awareness and knowledge of digital citizenship practices in a distance learning environment: case study" by [4] presents a comprehensive examination of the awareness and knowledge levels regarding digital citizenship among students and faculty in a distance learning context. The authors effectively synthesize findings from various empirical studies to highlight significant gaps in digital citizenship competencies, which are crucial for fostering a robust cybersecurity culture.

The article identifies nine key elements of digital citizenship, including etiquette, communication, and access, and emphasizes that a lack of knowledge in these areas serves as a critical indicator of insufficient engagement with technology ([4]). This observation is particularly relevant when considering the context of cybersecurity, as understanding digital citizenship is foundational to developing responsible online behaviors and practices.

Moreover, the article discusses findings from several studies, including those by Al-Abdullatif and Gameil (2020) and Elmali et al. (2020), which reveal a concerning gap in knowledge and practical application of security measures among students. The results indicate that while students may possess a general awareness of digital citizenship, their understanding of specific aspects such as digital rights, responsibilities, and security is lacking. This gap is critical, as it suggests that students may not be adequately equipped to navigate the complexities of the digital landscape safely.

[4] also highlight the comparative analysis conducted by Grammon (2020), which found no statistically significant differences in digital citizenship perceptions between online students and teachers. This finding raises questions about the effectiveness of current educational strategies in promoting digital citizenship, suggesting a need for targeted interventions that address both students and faculty to foster a more cohesive understanding of digital practices.

The article "Cyber Security Threat Awareness Framework for High School Students in Qatar" by [5] presents a comprehensive framework aimed at enhancing cybersecurity awareness among high school

students. The authors argue that the development of qualified individuals who are knowledgeable in cybersecurity is crucial for future decision-making in technology. This perspective underscores the importance of instilling a robust cybersecurity culture in students, who will ultimately become the leaders of technological evolution.

The article outlines three primary approaches to delivering cybersecurity awareness in educational settings, which are critical for addressing the prevalent ignorance regarding cybersecurity in school curricula. The first approach, the Conventional Delivery Method, utilizes both electronic and paper resources to disseminate important cybersecurity messages. This method includes strategies such as posters in cafeterias that remind students about the significance of safeguarding personal passwords. The effectiveness of this approach lies in its ability to reach students in common areas, thereby reinforcing key concepts in an engaging manner.

The second approach discussed is the use of educational videos. The authors highlight that videos serve as powerful tools for persuasion and understanding, particularly in conveying complex cybersecurity concepts. The London Digital Security Centre's initiative to produce educational videos is cited as an exemplary practice, focusing on critical topics such as the treatment of personal information, phishing attacks, and self-protection in contexts like bring-your-own-device (BYOD) policies and social media use. This multimedia approach not only caters to diverse learning styles but also enhances retention of information through visual engagement.

Lastly, the article introduces a game development learning model as a novel method for simulating cybersecurity activities. This approach aligns with contemporary educational trends that advocate for experiential learning, where students actively participate in scenarios that mimic real-world challenges. By engaging students in this interactive manner, the authors suggest that such simulations can significantly bolster their understanding of cybersecurity threats and appropriate responses.

The article "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy" by [6] provides a thorough examination of the critical role that cybersecurity awareness plays not only for cybersecurity specialists but also for operational managers within various organizations. This perspective is particularly relevant in a landscape where remote work has become commonplace, necessitating a shift in how cybersecurity threats are understood and mitigated.

One of the key insights from the study is the necessity for comprehensive training programs that equip employees with the skills to address cybersecurity threats arising from everyday activities, such as downloading files or updating devices. This finding underscores the importance of integrating cybersecurity training into the routine operations of organizations, rather than relegating it to a specialized function. The authors argue that cybersecurity leaders must remain vigilant and adaptable to the evolving nature of business environments, which is a critical aspect of maintaining a robust cybersecurity posture.

The research highlights a significant gap in the existing literature regarding Cybersecurity Awareness Capabilities (CSAC), noting that much of the available research does not provide a nuanced understanding of how knowledge and behavior regarding cybersecurity awareness differ across various demographics and geographical locations. The study's findings reveal that while there is a correlation between cybersecurity knowledge and awareness, disparities exist based on factors such as gender and location. For instance, the authors identify a notable deficiency in cybersecurity knowledge among Polish medical professionals, suggesting an urgent need for targeted training initiatives in that sector.

Moreover, the article emphasizes the effectiveness of a comprehensive design strategy for enhancing cybersecurity awareness among employees, particularly in the banking sector. This approach appears to yield better results compared to less structured training methods. The authors also address the moderate level of cybersecurity awareness among parents regarding the protection of their children from online threats, indicating a broader societal issue that requires attention.

The article "Adopting the Cybersecurity Concepts into Curriculum: The Potential Effects on Students Cybersecurity Knowledge" by [7] presents a critical examination of the current state of cybersecurity awareness among students and proposes a structured approach to enhance this awareness through curriculum integration. The authors highlight the increasing sophistication of cyberattacks and the alarming lack of knowledge among users regarding cybersecurity practices, which is particularly concerning in an era where digital learning has been accelerated by the COVID-19 pandemic.

The pilot study conducted by the authors is a significant contribution to understanding the existing levels of cybersecurity awareness among students enrolled in Information Security courses. The use of an online survey to gather data on various aspects of cybersecurity behavior—such as general knowledge, password security, and mobile security—provides a comprehensive overview of students' understanding and practices. The findings reveal a concerning gap in cybersecurity knowledge, which suggests that students are ill-equipped to protect themselves from potential cyber threats. This lack of awareness not only jeopardizes individual security but also poses broader risks to institutional data integrity.

The authors propose a four-step methodology to integrate cybersecurity concepts into non-security courses, which is a pragmatic approach given the constraints of existing curricula. By mapping existing content to the principles outlined in the Cybersecurity Community guideline (CSEC2017), the authors effectively identify gaps and suggest relevant topics to be included in the curriculum. This method not only enhances the relevance of cybersecurity education but also aligns with the need for a more interdisciplinary approach to teaching these critical concepts.

One of the strengths of this article is its emphasis on the collaborative role of universities in fostering a culture of cybersecurity awareness. The authors argue that by embedding cybersecurity principles into a broader range of courses, educational institutions can play a pivotal role in shaping students' understanding and behaviors regarding cybersecurity. This proactive approach is essential in a landscape where the responsibility for cybersecurity increasingly falls on individual users.

However, while the article provides a valuable framework for integrating cybersecurity concepts into the curriculum, it would benefit from a more detailed discussion on the implementation challenges that educators may face. Factors such as faculty training, resource allocation, and the need for ongoing assessment of the program's effectiveness are crucial for the successful adoption of the proposed methodology. Additionally, the article could explore how to engage students more effectively in the learning process, ensuring that the infusion of cybersecurity concepts is not merely theoretical but translates into practical skills and behaviors.

3. Conclusion

The literature on assessing students' cybersecurity culture through digital platforms reveals a critical understanding of the multifaceted nature of cybersecurity awareness and education. The introduction highlights the growing importance of cybersecurity in a digital age, particularly among students who will be future decision-makers. The studies reviewed emphasize the need for individuals to take an active role in their cybersecurity practices, moving beyond the perception that security is solely the

responsibility of specialists [1]. The concept of security culture is explored extensively, with an emphasis on the role of organizational norms, values, and subcultures in shaping security behaviors [2]. It is evident that fostering a robust security culture requires a collective effort, with champions within organizations advocating for cybersecurity awareness and ethical behavior [3]. The educational context is particularly significant, as studies indicate substantial gaps in digital citizenship knowledge among students and faculty, underscoring the need for enhanced training in digital law and safety [4]. Moreover, tailored approaches to cybersecurity education, such as the cybersecurity threat awareness framework for high school students in Qatar, highlight the importance of engaging students through diverse educational strategies, including conventional methods, educational videos, and game-based learning [5]. The necessity for comprehensive training that extends beyond cybersecurity personnel to include operational managers is also emphasized, particularly in the context of remote work [6]. Finally, integrating cybersecurity concepts into academic curricula is crucial for enhancing students' awareness and understanding of cybersecurity risks and protective measures [7]. The proposed methodologies for curriculum integration not only aim to bridge the knowledge gap but also promote a culture of security awareness among students. In conclusion, the reviewed literature collectively underscores the critical need for a comprehensive approach to assessing and enhancing students' cybersecurity culture through digital platforms. It highlights the importance of individual engagement, organizational culture, educational strategies, and curriculum integration in fostering a secure digital environment for students.

References

1. A. Respicio, "SECURITY PRACTICES: KEEPING INDIVIDUALS SAFE AND AWARE IN THE CYBER WORLD," 2019. [PDF]
2. A. Ertan, G. Crossland, C. Heath, D. Denny et al., "Cyber Security Behaviour In Organisations," 2020. [PDF]
3. B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," 2021. [PDF]
4. M. Hawamdeh, Z. Altınay, F. Altınay, A. Arnavut et al., "Comparative analysis of students and faculty level of awareness and knowledge of digital citizenship practices in a distance learning environment: case study," 2022. ncbi.nlm.nih.gov
5. M. Al-Tajer and R. Adeyemi Ikuesan, "Cyber Security Threat Awareness Framework for High School Students in Qatar," 2022. [PDF]
6. S. Akter, M. Rajib Uddin, S. Sajib, W. Jin Thomas Lee et al., "Reconceptualizing cybersecurity awareness capability in the data-driven digital economy," 2022. ncbi.nlm.nih.gov
7. M. Azzeh, A. Mousa Altamimi, M. Albashayreh, and M. A AL-Oudat, "Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge," 2022. [PDF]