A Latent Profile Analysis of Middle School Students' Cyber Resilience: Educational Implications Based on NIST Framework

Soylu, E., İstanbullu, A., & Delialioğlu, Ö.

cybersecurity Digital Citizenship Online Safety

This study classifies middle school students' cyber resilience (CR) levels using Latent Profile Analysis based on the NIST Cybersecurity Framework. Data from 2,483 Turkish middle school students revealed four distinct profiles: Advanced CR, Intermediate CR, Low CR, and Developing CR. Results showed that prior exposure to cybersecurity threats significantly influenced resilience levels, while gender differences were non-significant. The findings emphasize the need for differentiated, profile-based educational interventions. For the Low CR Profile, basic concepts and risk recognition are prioritized. The Developing CR Profile focuses on data protection strategies. The Intermediate CR Profile includes threat detection and security monitoring. The Advanced CR Profile emphasizes incident response and recovery strategies. By implementing adaptive learning platforms tailored to students' resilience profiles, educators can better equip students with essential cybersecurity skills for navigating the digital landscape safely and effectively.

Introduction

Educational technologies have made learning processes more accessible, flexible, and interactive. However, they have also increased students' exposure to cybersecurity risks. Cyber threats, online privacy risks, and students' ability to navigate the digital world safely present significant challenges (Quayyum et al., 2021). Due to their developmental characteristics, students in this age group struggle to recognize online threats and develop effective defense strategies. Therefore, it is crucial to provide them with the necessary support against digital threats (Marciano et al., 2020; Yang et al., 2021). To enhance students' cyber resilience (CR), it is essential to assess their current awareness levels and develop tailored educational content accordingly.

The ISTE Student Standards (ISTE, 2021) emphasize the importance of students acquiring skills such as digital citizenship, critical thinking, and safe internet use. However, to ensure the effective acquisition of these skills, personalized and adaptive educational approaches should be adopted based on students' CR levels. Generic educational content may overlook students' individual awareness levels and learning needs, thereby hindering the effectiveness and sustainability of learning processes. Consequently, directing students toward profile-based educational content will enhance their awareness of digital threats and contribute to their CR.

Existing research indicates that students' exposure to online risks is increasing and that stronger educational interventions are required to help them cope with these challenges (Slyusar et al., 2024; Lewin et al., 2021; Milosevic & Doric, 2023; Ragni et al., 2022; Koç, 2024). The European Kids Online Report highlights the need for more robust protection mechanisms against online

threats for children (Livingstone et al., 2011). However, cybersecurity education often provides students with standardized and generic content, disregarding their individual awareness levels and developmental needs (Staksrud, 2016).

This study aims to classify students' CR levels based on the NIST Cybersecurity Framework (NIST CSF) and the security-related sub-dimensions of the Digital Competence Framework (DigiComp 2.2). Four distinct student profiles—beginner, intermediate, developing, and advanced—were identified. By tailoring educational content according to these profiles, the study seeks to provide students with personalized and goal-oriented learning experiences. This approach not only enhances students' CR but also fosters the development of individuals who are conscious, proactive, and equipped with a sustainable understanding of cybersecurity in the digital world.

The study addresses the following research questions:

1. How can middle school students' CR levels be classified?
2. How are students' demographic characteristics (e.g., gender, grade level, and internet usage duration) related to their CR profiles?
3. How can these profiles be utilized to develop more effective digital security education for middle school students?

By answering these questions, the study aims to contribute to the development of more effective and personalized cybersecurity education programs that align with students' individual learning needs and resilience levels.

Method

Research Design

In this study, the survey research method, one of the quantitative research methods, was employed.

Participants

A total of 2,483 middle school students from public schools in Turkey participated in this study, with 55.9% (n = 1,389) being female and 44.1% (n = 1,094) being male. Regarding grade levels, 35.0% (n = 868) were in 7th grade, 31.6% (n = 784) in 6th grade, 31.2% (n = 774) in 8th grade, and 2.2% (n = 57) in 5th grade.

Data Collection Tool

The data were collected online via Google Forms using the CR Scale (CRS) between October and December 2024, ensuring accessibility and ease of participation for students. This study is supported by TÜBİTAK under the project code 2218-122C266.

The CR Scale (CRS): The data collection instrument was developed by İstanbullu et al. (2025) based on the NIST CSF. The scale consists of five factors (Identification, Protection, Detection, Response, and Recovery) and includes a total of 43 items, utilizing a 5-point Likert scale (Strongly Disagree - Strongly Agree) as an assessment tool. The Cronbach's Alpha coefficient for the overall scale was found to be 0.89, while the reliability coefficients for the sub-dimensions ranged between 0.81 and 0.87. These findings indicate that the scale is a valid and reliable instrument for measuring CR.

Data Analysis

In this study, Latent Profile Analysis (LPA) (RQ1), ANCOVA (Covariate Analysis-LPA BCH) (RQ2), and Descriptive Analysis (RQ3) were conducted to address the research questions. All analyses were performed using SPSS 27 and Mplus 8 software.

Results

The Latent Profile Analysis (LPA) conducted to classify middle school students' CR levels identified a four-profile model as the most appropriate solution. This model demonstrated high classification accuracy (entropy = 0.957), significant LMR and BLRT test results ($p < 0.0000$), and an acceptable minimum subgroup proportion (8.1%). Although the five-profile model exhibited lower information criterion values, it was not selected due to its smallest subgroup proportion (3.8%) falling below the acceptable threshold of 5%. The distribution of students across the four identified profiles is as follows: Advanced CR Profile (n = 403), Intermediate CR Profile (n = 314), Low CR Profile (n = 230), and Developing CR Profile (n = 78). These profiles reflect students' competency levels in identifying, protecting, detecting, responding to, and recovering from cyber threats, aligning with the different stages of the NIST CSF.

The Block, Crons, and Hagenaars (BCH) method was employed to examine the relationship between students' demographic characteristics and their CR profiles. The Advanced CR Profile was set as the reference group, and the covariate analysis results indicated that gender did not have a significant effect on profile membership. However, exposure to cyber threats significantly predicted students' profile membership ($p<.05$). The effect of cyber threat exposure on profile membership varied across profiles, with significant differences observed for the Low (0.000), Developing (0.005), and Intermediate (0.043) CR Profiles. Additionally, it was found that profiles 1 and 2 scored below the population mean for all indicator variables, whereas profiles 3 and 4 scored above the population mean.

The content analysis conducted to determine CR profile-specific educational content for middle school students highlights how each stage of the NIST Cybersecurity Framework can be tailored to different profiles. The proposed instructional content for each profile is designed to provide gradual progression, taking into account students' current competency levels. In particular, transition strategies between profiles identify specific focus areas that facilitate students' advancement to higher resilience levels. The analysis results emphasize the necessity of differentiated educational content across profiles. For the Low CR Profile, the focus is on fundamental concepts, safe device usage, and risk recognition. The Developing CR Profile includes data protection strategies and preventive security measures. The Intermediate CR Profile incorporates advanced threat detection and security monitoring, while the Advanced CR Profile emphasizes incident response skills and recovery strategies. Additionally, scaffolded learning strategies have been identified to support seamless profile transitions and foster progressive skill development.

Discussion and Recommendations

The findings indicate that middle school students exhibit varying levels of CR based on NIST stages. While a considerable portion demonstrates Intermediate or Advanced CR, suggesting a stronger grasp of digital safety practices, a significant number of students fall into the Basic or Developing CR categories, indicating limited preparedness against cyber threats. However, given the multifaceted nature of CR, students across all profiles require targeted educational interventions aligned with NIST stages to enhance their ability to prevent, detect, respond to, and recover from cyber risks effectively.

Additionally, prior exposure to cybersecurity threats was found to significantly influence resilience levels, suggesting that real-world encounters with cyber risks may serve as learning experiences for students. Interestingly, gender differences were found to be non-significant, indicating that both male and female students exhibited similar patterns of cybersecurity resilience. This contrasts with some previous studies that have suggested gender-based differences in cybersecurity awareness and engagement. These findings emphasize the need for further research into the factors that contribute to cybersecurity education effectiveness.

Furthermore, adaptive learning platforms that tailor content to students' resilience profiles should be integrated into digital education strategies. Future research should explore the long-term impact of cybersecurity training programs and investigate

additional demographic factors that may influence CR. By implementing these targeted interventions, educators and policymakers can better equip students with the necessary skills to navigate the evolving digital landscape safely and effectively.

References

Ciuchi, C. (2022). Developing a Comprehensive Model for Digital Lifelong Learning Using Cyber Resilience Framework. *International Conference on Cybersecurity and Cybercrime*, *9*, 105–112. https://doi.org/10.19107/CYBERCON.2022.14

Koç, E. S. (2024). Fostering mental-wellbeing and health behavior among students through digital literacy interventions. *American Journal of Health Behavior, 48*(4), 1039-1048. https://doi.org/10.5993/ajhb.48.4.14

Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and Responsible Internet Use in a Connected World: Promoting Cyber-Wellness. *Canadian Journal of Learning and Technology*, *47*(4). https://doi.org/10.21432/cjlt28069

Lin, Y., & Zhang, J. (2024). Educational resilience in the digital age: The path of technological empowerment in higher education in the post-pandemic era. *Advances in Vocational and Technical Education, 6*(1), Article 1. https://doi.org/10.23977/avte.2024.060122

Milosevic, M., & Doric, B. (2023). *Rebuilding stronger: Students' digital resilience post-pandemic*. eLearning.

Ragni, B., & Guerrini, P. (2022). Digital resilience and psychological wellbeing in education: Addressing online risks. *Proceedings of TIE 2022*, 431-437. https://doi.org/10.46793/tie22.431r

Slyusar, V., Yablonska, N., Zayko, L., & Panchenko, N. (2024). Building digital resilience in the training of teachers and students. *Society and Security, 2-3*(3), 106-111. https://doi.org/10.26642/sas-2024-2-3(3)-106-111

Vuorikari, R., Kluzer, S., & Punie, Y. (with Europäische Kommission). (2022). *DigComp 2.2 - the digital competence framework for citizens: With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/115376

This work is released under a CC BY license, which means that you are free to do with it as you please as long as you properly attribute it.