ANALYZING PERFORMANCE PATTERNS AND USER EXPERIENCE IN ONLINE CYBERSECURITY CHALLENGES: INSIGHTS FROM SKRCTF

Khoo Li Jing [12], Maizatul Hayati Mohamad Yatim [1], and Wong Yoke Seng [1]

[1] Faculty of Computing and Meta-Technology, Sultan Idris Education University, Tanjong Malim, Malaysia
[2] School of Creative Media and Computing, University of Wollongong Malaysia, Jalan Kontraktor U1/14, Seksyen U1, 40150, Shah Alam, Selangor, Malaysia

ABSTRACT

The field of cybersecurity education has undergone a significant transformation, with the emergence of innovative e-learning platforms that aim to bridge the gap between academic institutions and industry. This study investigates the effectiveness of SKRCTF, a customized Capture-the-Flag platform designed to support cybersecurity skill development, through comprehensive analysis of user performance patterns and learning experiences. Drawing from data collected from 120 participants over a 12-week period, this research employs mixed-methods analysis to examine learning progressions, engagement patterns, and skill development pathways in cybersecurity education. The findings reveal three key insights: 1. the emergence of distinct specialist and generalist learning patterns, challenging traditional assumptions about linear skill progression; 2. the identification of an optimal engagement zone that maximizes learning effectiveness; and 3. the discovery that analytical challenges serve as effective entry points for cybersecurity skill development. The study also uncovers a complex relationship between perceived difficulty and learning outcomes, where higher perceived difficulty often correlates with increased persistence rather than decreased engagement. These insights contribute to both theoretical understanding of cybersecurity skill development and practical platform design considerations. The research suggests that effective cybersecurity education platforms should support multiple learning pathways, implement structured engagement mechanisms, and carefully sequence challenges to optimize skill development. These findings have significant implications for the design of cybersecurity education programs and the development of future security professionals.

KEYWORDS

Cybersecurity education, e-learning, skill development, learning analytics, performance patterns

1. INTRODUCTION

This study investigates SKRCTF, a customized Capture-the-Flag platform designed to support hands-on cybersecurity skill development. Existing cybersecurity training methods often struggle to cater to the diverse skill levels and backgrounds of participants, leading to suboptimal learning experiences [1].

1.1. Background and Research Context

The rise of cyber ranges has offered a more immersive and practical training approach in Malaysian universities, yet their resource-heavy nature restricts widespread accessibility [2]. This observation led us to explore more accessible alternatives such as CTF-style environments [3][4].

These platforms combine practical challenges with educational scaffolding, enabling learners to develop technical competencies in a controlled environment. However, current research shows limited evidence of their effectiveness in developing threat recognition and pattern identification skills [5].

We designed SKRCTF to address these gaps, offering a customizable e-learning platform that adapts to diverse learner backgrounds and skill levels. The key features of SKRCTF include:

- Gamified learning that simulates real-world scenario in a safe environment.
- Scaffolding and guided learning by providing structured learning paths and progressive challenge difficulties.
- Adaptive and personalized learning with data-driven performance tracking.
- Community-driven learning via peer-to-peer learning through discussion forums.

1.2. Platform Overview and Scope

SKRCTF encompasses the typical topics in cybersecurity education. The 12 categories were warm up tutorials, web security, cryptography, digital forensics, software reverse engineering (RE), binary exploitation, Open-Source Intelligence (OSINT), mini games, programming, steganography and miscellaneous. Each challenge category contains varying difficulty levels, with a total of 127 challenges. This study examines data from 120 participants aged 19-30 who engaged with the platform over a 12-week period.

1.3. Research Objectives and Questions

Previous research on the SKRCTF platform found limited evidence of learners recognizing cybersecurity threats and cryptography patterns, despite their involvement [6]. This study now shifts focus to investigating factors influencing learner motivation in the Malaysian cybersecurity education context. The research questions are:

1. What factors contribute to the variability in performance between high and low scorers?
2. How does perceived challenge difficulty relate to actual performance?
3. What demographic factors influence performance across challenge categories?
4. How do user expectations align with their platform experience?
5. What patterns emerge in challenge completion rates across different user groups

2. METHODOLOGY

To address these research questions, this study employed a mixed-method approach, combining quantitative and qualitative data analysis.

2.1. Data Collection

We collected survey data from learners using SKRCTF to train cybersecurity skills. We included a survey question as part of the challenges to measure the learners' perception and performance level. The study duration is between 1st August 2024 to 18th September 2024. Ethical considerations, such as data anonymization and informed consent, were followed.

2.1.1. Survey Design and Distribution

The survey consisted of four sections: demographic information, performance self-assessment, challenge difficulty perception, and learning strategy preferences. The survey was distributed after participants attempted 20 challenges through the SKRCTF platform, and participants were incentivized to complete the survey with points and virtual badges.

2.1.2. Performance Data Collection

The researcher recorded the participants' performance data, including the number of challenges completed, number of challenge categories completed, and total attempts taken to complete each challenge.

2.2. Data Analysis Techniques

Descriptive statistics were employed to summarize participant demographics, challenge completion rates, and overall performance metrics. Correlation analysis, specifically Pearson's correlation coefficient, was used to examine relationships between perceived difficulty and performance, as well as inter-category performance correlations. Comparative analysis was conducted to assess performance differences across demographic groups and difficulty perception categories. Frequency analysis and cross-tabulation were utilized to examine the distribution of responses across various categorical variables.

Thematic analysis was employed to categorize and interpret participants' suggestions for platform improvement. Content analysis was used to identify recurring patterns and themes in participants' feedback and experiences.

3. FINDINGS

The collected data and analysis, based on the 5 research questions, led to the identification of 2 main themes: 1) Progressive learning patterns; and 2) Performance-Engagement dynamics. The research questions were then mapped to these developed themes.

3.1. Progressive Challenge Design and Skill Development

The data showed that the learning curve on the SKRCTF platform was not linear but follow distinct patterns across challenge categories and participant types. Analysis on the completion aretes and engagement patterns led to 3 key findings: natural learning progression, specialized skill development paths, and optimal engagement zones.

3.1.1. Natural Learning Progression

Completion rates across challenge categories revealed a clear skill progression hierarchy. The categories difficulty tiers are: 1. Entry level (>40% average completion rate): Warm up (54.46%), OSINT (83.33%), Forensics (47.19%), Linux (44.64%); 2. Intermediate Level (25-40% average completion): Web (29.83%), Crypto (33.51%), Steganography (35.42%), Binary (29.17%); 3. Advanced Level (<25% average completion): Programming (12.50%), Misc (14.17%).

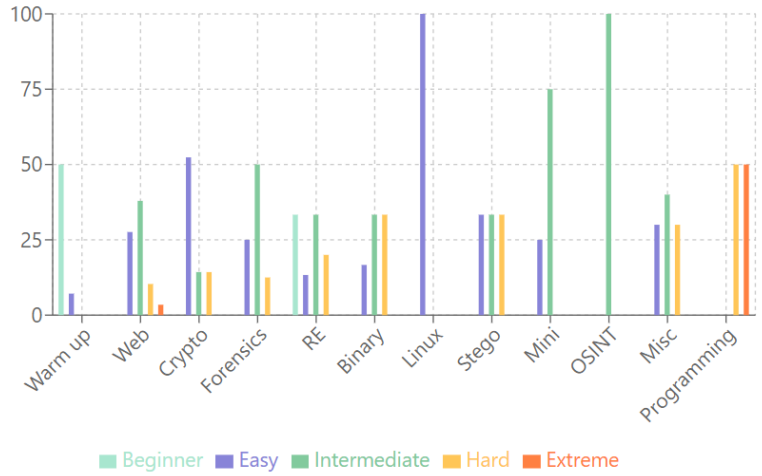

Figure 1. Challenge distribution and difficulty level.

Increased practice attempts do not directly translate to greater learning effectiveness, shown in Figure 2. The scatter plot shows a weak positive correlation between the number of attempts and the completion rate. Even among participants with similar attempt counts, there is substantial variability in their completion rates. Interestingly, the highest average completion rate of 52.1% is observed within the 101-150 attempt range. This aligns with prior research [7], which indicates that the effectiveness of learning cybersecurity skills is enhanced by an environment that encourages active participation and structured learning, rather than just repetitive practice.

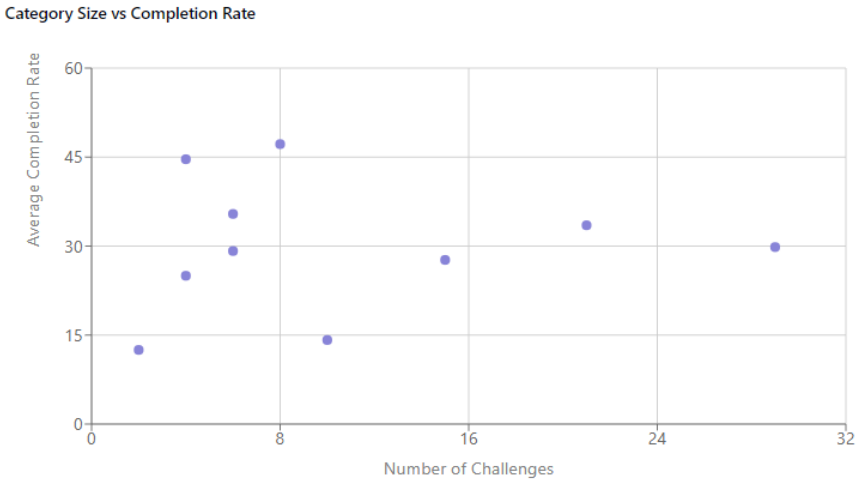

Figure 2. Average completion rate against category size

The number of challenges attempted decreases as difficulty increases, suggesting a natural learning curve [8][9]. Learners tend to be more successful in completing entry-level challenges compared to advanced ones. Beginning with easier challenges can help build learners' confidence, which may then lead to increased engagement and attempts at higher-difficulty challenges.

The challenge categories reveal a weak negative correlation between category size and completion rates. Larger categories tend to have lower average completion rates, though some exceptions exist. Categories with many challenges show this negative correlation, while medium-

sized categories have varied completion rates. Further analysis based on prior research [10], the categories can be classified into three types: Technical, Analytical, and Mixed. Figure 3 presents the new group type and their distribution of difficulty and completion rates.

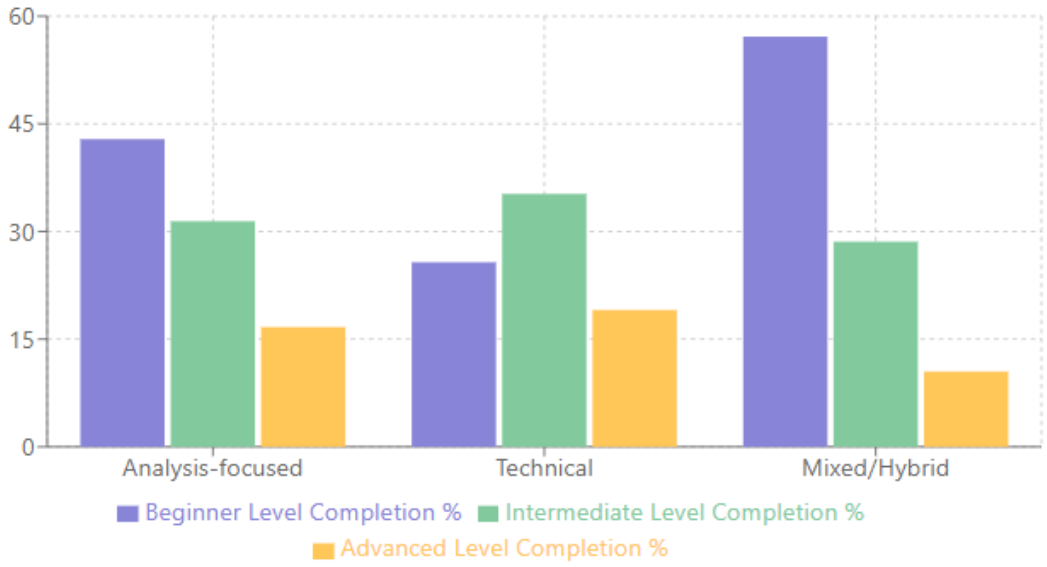

Figure 3. Challenge categories and completion rate for each difficulty level

The Technical category, which includes Web Exploitation, Reverse Engineering, Binary Exploitation, and Programming, exhibited the lowest average completion rates (27.98%). In contrast, the Analytical category, such as Digital Forensics, Open-Source Intelligence, Cryptography, and Steganography, demonstrated the highest completion rates (46.74%). The remaining Mixed category, requiring cross-domain skills including Warm-up, Linux, Mini Games, and Miscellaneous, had an average 36.70% completion rate.

The Analytical and Mixed categories have higher completion rates for beginners at 42.86% and 57.14% respectively, but the rates gradually decline at higher difficulty levels. This suggests that the entry points for these categories effectively engage learners but may require better support for progression. In contrast, the Technical category has a lower beginner completion rate but higher rates at the intermediate level, showing a more consistent progression through higher difficulty levels. This indicates that the Technical category builds upon foundational skills with steady development, providing an effective learning curve for more experienced participants, but may be more intimidating for beginners. [11].

The relationship between challenge type and completion rates offers valuable insights for designing learning progressions in cybersecurity education. This pattern suggests that analytical challenges provide better entry points for beginners, while technical challenges require more structured scaffolding but enable consistent skill development [12][13].

3.1.2. Specialist and Generalist Development

Analysis of individual learning trajectories revealed two distinct learner profiles: Specialists (n=62), who achieved high performance with over 70% completion in specific categories; and Generalists (n=46) maintained consistent performance of over 40% completion across multiple categories. The remaining 54% displayed a mix of performance patterns.

Diving deeper into each performance characteristics, Specialists required an average of 1.92 attempts per success in their dominating category while Generalists averaged 1.85 attempts per success across all categories. These patterns suggest differences in their learning strategies [14] [15]. Specialists may focus on developing deep expertise within a particular domain, while Generalists adopt a broader, cross-disciplinary approach. Specialists tend to have higher success rates in advanced challenges within their specialty, while Generalists may exhibit greater adaptability across different challenge types. Recognizing these distinct learner profiles can guide the design of personalized learning pathways and support mechanisms, moving beyond a one-size-fits-all approach.

3.2. Performance-Engagement Dynamics

Analysis reveals a complex relationship between participants' perceived difficulty, engagement patterns, and actual performance on the SKRCTF platform. Perceived difficulty reliably indicates performance while revealing interesting engagement and persistence patterns.

3.2.1. Perceived Difficulty-Performance Patterns

The correlation between perceived challenge difficulty and performance exhibited significant yet nuanced patterns. A moderate negative correlation (-0.421) emerged between perceived difficulty and average scores, with performance varying by difficulty perception: "Easy peasy" had the highest average overall completion (36.75%); "Somehow challenging" performed second-best (31.52%); "Quite challenging" group had an average performance of 27.55%; "Very challenging" group had the lowest average performance (22.92%).

However, perceived difficulty showed unexpected relationships with engagement. Participants rating challenges as "Very challenging" made significantly more attempts (average 107.4) compared to those rating them "Easy peasy" (average 72.9). This suggests that higher perceived difficulty often motivated deeper engagement rather than deterring participation. This aligns with the learning progression where practitioners often start with a broad approach before gradually specializing [16]. As these participants gain more experience, their self-awareness and metacognitive abilities improve, leading to a better alignment between their perceived difficulty and actual performance.

3.2.2. Optimal Engagement Zones

The weak positive correlation between attempts and completion rates combined with the variability in success rates among participants with similar attempt counts, suggests that effective learning depends more on approach strategy than persistence alone. This aligns with findings from [17] about the importance of balancing challenge and skill for optimal engagement.

Figure 4 shows that the 101-150 attempt range is the most optimal engagement zone across the 127 total challenges, achieving 52.1% completion rate. This finding challenges the assumption that more practice automatically leads to better outcomes. The data indicates that the importance of structured, measured practice yields better results over raw attempt numbers. Building on prior research [18], the different challenge categories exhibited distinct patterns in learner engagement. Technical challenges demonstrated lower overall completion rates but consistent progression through increasing difficulty levels, while analytical challenges had higher initial accessibility but varying progression patterns.

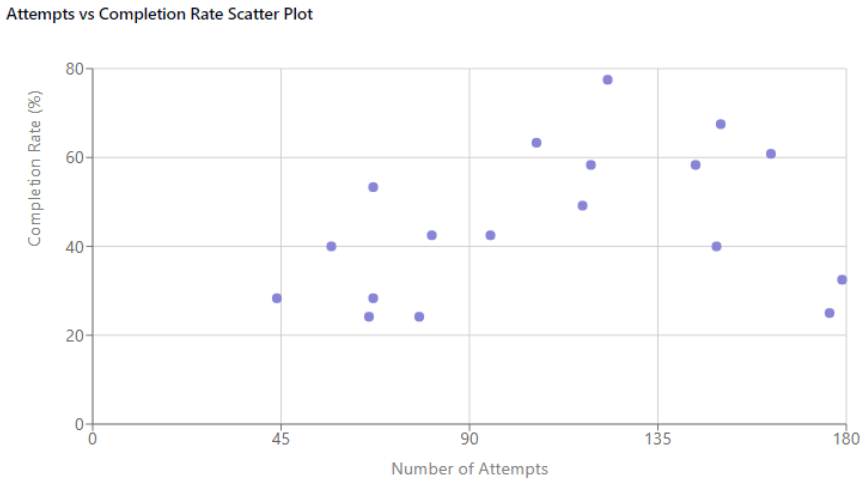

Figure 4. Attempt vs completion rate scatter plot

Different challenge types require tailored engagement strategies. This indicates a need for more effective category-specific learning strategies than uniform approaches. The data suggests diminishing returns after certain thresholds, highlighting the importance of designing engagement mechanisms that encourage regular, measured practice rather than intense bursts. Harnessing these insights, learning platforms can integrate adaptive analytics to steer learners towards more productive practice strategies and better long-term outcomes.

4. DISCUSSION

The data-driven insights gathered from the SKRCTF platform can help inform the development of innovative e-learning models optimized for effective cybersecurity skill acquisition. Though the 5 research questions did not uncover notable distinctions in demographic factors, we explore the pivotal theoretical insights and practical applications of the findings, with a view toward the broader vision of enhancing cybersecurity education framework development.

4.1. Theoretical Implications

Research in technical education has demonstrated the potential of Capture-the-Flag activities to improve student engagement and self-efficacy in computing domains [14] [1]. Our findings extend this understanding by revealing how the SKRCTF platform supports different learning pathways while fostering sustained engagement. The complex relationship between perceived difficulty and learning outcomes suggests a "confidence-competence spiral" where initial success in general skill categories, particularly analytical challenges, builds the foundation for tackling more technical domains.

The identification of distinct specialist and generalist learning patterns offers a novel conceptual framework for comprehending skill development in cybersecurity skill development. This dual-path framework challenges traditional models of linear progression [19][20], suggesting that effective platforms must support both deep domain expertise and broad skill acquisition. The divergent attempt patterns observed between specialists and generalists suggest fundamentally diverse learning strategies, challenging the conventional one-size-fits-all approach in cybersecurity education.

Our analysis challenges the assumption on increased practice automatically leads to improved performance in cybersecurity education. The optimal engagement zone suggests a more complex relationship between effort and achievement. The stark difference in completion rates between technical and analytical categories reveals a fundamental distinction in how these skills are acquired with analytical skills potentially laying the foundation to technical competency. This insight is significant given that participants who perceived challenges as more difficult showed higher persistence, serving as a motivator rather than a deterrent in self-directed learning environment.

4.2. Practical Implication

The findings from SKRCTF provide concrete guidance for designing cybersecurity learning platforms. The clear differentiation in completion rates between technical and analytical categories suggests that platforms should intentionally sequence challenges to build learner confidence. Starting with analytical challenges that demonstrate higher accessibility before introducing technical challenges can create more progressions while building learner confidence.
Entry point planning across each cybersecurity challenge category is crucial. Well-designed introductory challenges showed more consistent engagement patterns, suggesting that careful attention to initial challenge design is crucial for learner retention. This extends beyond simple difficulty ratings to include consideration of required background knowledge and skill prerequisites. The distinct engagement patterns between specialists and generalists underscore the need for flexible support systems. Specialized deep-dive resources should be available for specialists, while generalists should be provided with broader contextual connections to enhance their learning.

The optimal engagement zone could be a transformative guide for instructional design, suggesting a need for more sophisticated gamification beyond basic points and badges in cybersecurity education. Platforms should implement analytics-driven mechanisms on supporting sustained, meaningful engagement rather than maximum attempt numbers. Understanding the relationship between perceived difficulty and engagement patterns can help determine appropriate reward structures, support diverse engagement styles, provide meaningful feedback, and encourage strategic practice patterns.

4.3. Educational Framework Development

SKRCTF and associated research findings contribute to the emerging field of cybersecurity education by providing a data-driven framework for designing effective e-learning systems.
The identification of distinct specialist and generalist learning patterns [18] [8] offers a novel conceptual model for understanding skill development in cybersecurity education. The observed progression from analytical to technical challenges aligns with established educational principles of scaffolded learning while addressing practical cybersecurity skills.

A proposed integration framework includes:

- Using analytical challenges (forensics, cryptography) to introduce core concepts
- Gradually incorporating technical challenges (web security, reverse engineering) to build practical skills
- Leveraging OSINT and steganography challenges to develop investigative thinking
- Employing binary exploitation and programming challenges for advanced skill development

A balanced skill development model recognizes that effective cybersecurity education must foster both depth and breadth of knowledge. The SKRCTF case study showcases how data-driven insights can inform the design of flexible, adaptive curricula to cater to the diverse needs of learners. The framework features core components starting with foundational skills common to all tracks, as well as specialized deep-dive opportunities. It also incorporates cross-domain integration projects with industry-aligned challenge scenarios. This underscores the importance of enabling learners to develop along their natural inclinations while ensuring baseline competency across essential domains.

Despite the current SKRCTF platform having limited sample size and demographic constraints, we propose an integrated assessment framework that combines formative and summative evaluations based on the platform's engagement patterns and performance metrics. Analyzing learners' attempt patterns and problem-solving approaches across different skill domains can provide meaningful feedback to both educators and learners, informing their respective improvement efforts.

While maintaining pedagogical rigor, bridging academic learning to industry needs remains a critical priority. Besides mapping challenges to learning outcomes and producing metrics for skill evaluation, developing industry-relevant tools and techniques, supporting continuous professional development are paramount in preparing the next generation of cybersecurity professionals.

5. LIMITATIONS AND FUTURE RESEARCH

The preliminary research conducted on the SKRCTF platform represents an initial step in understanding how adaptive e-learning can transform cybersecurity education. Limitations include the relatively small sample size, limited time frame, homogeneous demographic, self-reported difficulty perception.

To further enhance the SKRCTF platform, future research should focus on expanding the range of learners, incorporating diverse challenge types, and conducting longitudinal studies to track skill development over time. While SKRCTF provides a robust foundation for cybersecurity education, certain platform-specific limitations should be acknowledged, such as the distribution of challenges across categories, the need for a more sophisticated implementation of scaffolding mechanisms, and the development of more nuanced assessment metrics.

Several promising research directions arise from this work, including learning analytics [19], cross-platform integration, and cognitive load analysis. These areas could warrant further investigation into adaptive learning systems, team learning dynamics, industry impact, and cultural factors. Specifically, future research could explore the application of learning analytics to gain deeper insight into specialist-generalist learning patterns and performance on the SKRCTF platform. Cross-platform integration could enable the sharing of resources and best practices across different cybersecurity education initiatives, fostering a more collaborative and comprehensive approach to curriculum development [20]. Cognitive load analysis could provide valuable insights into the relationship between perceived difficulty, actual complexity, and learning outcomes, informing the design of more effective instructional strategies and challenge sequences [21]. Additionally, investigations into team learning dynamics and the impact of cultural factors on cybersecurity education could lead to the development of more inclusive and supportive learning environments. Exploring these research directions could significantly enhance the design and implementation of adaptive learning systems for the cybersecurity field.

6. CONCLUSION

This study provides valuable insights into the design and implementation of effective cybersecurity education platforms through a comprehensive analysis of the SKRCTF platform. The research reveals several key findings that contribute to our understanding of how learners engage with and develop cybersecurity skills in an online environment.

First, the identification of distinct learning patterns, particularly the emergence of specialist and generalist approaches, challenges the traditional assumptions about linear skill progression in cybersecurity education. This suggests that effective platforms must support multiple learning pathways while maintaining core competency development across essential domains.

Second, the research demonstrates a complex relationship between perceived difficulty, engagement patterns, and learning outcomes. The discovery of an optimal engagement zone and the observation that higher perceived difficulty often correlates with increased persistence rather than decreased engagement provides valuable guidance for platform design and pedagogical approaches.

Third, the analysis of category-based learning patterns reveals that analytical challenges may serve as an effective entry point for cybersecurity education, with technical challenges requiring more structured support and scaffolding. This insight can inform the design of more effective learning progressions in cybersecurity education platforms.

While this study has limitations, including sample size and demographic constraints, it provides a foundation for future research in cybersecurity education. Future studies should explore longitudinal learning patterns, investigate team-based learning dynamics, and examine the impact of cultural factors on cybersecurity skill development. This research contributes to the ongoing development of evidence-based approaches to cybersecurity education, ultimately supporting the preparation of the next generation of cybersecurity professionals.

ACKNOWLEDGEMENTS

The authors would like to thank Sultan Idris Education University for final support for this research. The first author would also like to appreciate the research support provided by University of Wollongong Malaysia during his research attachment when this article was written.

REFERENCES

[1] M. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, “Cyber range design framework for cyber security education and training,” Mar. 18, 2023, Springer Science+Business Media. doi: 10.1007/s10207-023-00680-4.

[2] P. Šeda, J. Vykopal, V. Švábenský, and P. Čeleda, “Reinforcing Cybersecurity Hands-on Training With Adaptive Learning,” Oct. 13, 2021. doi: 10.1109/fie49875.2021.9637252.

[3] M. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, “Cyber range design framework for cyber security education and training,” Mar. 18, 2023, Springer Science+Business Media. doi: 10.1007/s10207-023-00680-4.

[4] K. Leune and S. J. Petrilli, “Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education,” Sep. 27, 2017. doi: 10.1145/3125659.3125686.

[5] T. Goodman and A.-I. Radu, “Learn-Apply-Reinforce/Share Learning: Hackathons and CTFs as General Pedagogic Tools in Higher Education, and Their Applicability to Distance Learning,” Jan. 01, 2020, Cornell University. doi: 10.48550/arxiv.2006.04226.

[6] O. Chernikova, N. Heitzmann, M. Stadler, D. Holzberger, T. Seidel, and F. Fischer, "Simulation-Based Learning in Higher Education: A Meta-Analysis," Jun. 15, 2020, SAGE Publishing. doi: 10.3102/0034654320933544.

[7] L. J. Khoo, "Design and Develop a Cybersecurity Education Framework Using Capture the Flag (CTF)," Jun. 12, 2018, IGI Global. doi: 10.4018/978-1-5225-6026-5.ch005.

[8] P. L. da R. Rodrigues, L. P. Franz, J. F. P. Cheiran, J. P. S. da Silva, and A. S. Bordin, "Coding Dojo as a transforming practice in collaborative learning of programming," Sep. 18, 2017. doi: 10.1145/3131151.3131180.

[9] B. Grawemeyer, J. Halloran, M. England, and D. Croft, "Feedback and Engagement on an Introductory Programming Module," Dec. 27, 2021. doi: 10.1145/3498343.3498348.

[10] B. Yett, C. R. Snyder, N. Hutchins, and G. Biswas, "Exploring the Relationship Between Collaborative Discourse, Programming Actions, and Cybersecurity and Computational Thinking Knowledge," Dec. 08, 2020. doi: 10.1109/tale48869.2020.9368459.

[11] M. H. Dunn and L. D. Merkle, "Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests," Feb. 21, 2018. doi: 10.1145/3159450.3159462.

[12] J. Msane, B. M. Mutanga, and T. Chani, "Students' Perception of the Effect of Cognitive Factors in Determining Success in Computer Programming: A Case Study," Jan. 01, 2020, Science and Information Organization. doi: 10.14569/ijacsa.2020.0110724.

[13] K. Aguar, S. Safaei, H. R. Arabnia, J. B. Gutiérrez, W. D. Potter, and T. R. Taha, "Reviving Computer Science Education through Adaptive, Interest-Based Learning," Dec. 01, 2017. doi: 10.1109/csci.2017.202.

[14] V. Švábenský et al., "Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises," Feb. 22, 2022. doi: 10.1145/3478431.3499414.

[15] M. Ellis, L. Baum, K. Filer, and S. H. Edwards, "Experience Report: Exploring the Use of CTF-based Co-Curricular Instruction to Increase Student Comfort and Success in Computing," Jun. 18, 2021. doi: 10.1145/3430665.3456376.

[16] R. W. Bell, E. Y. Vasserman, and E. C. Sayre, "Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses," Jul. 08, 2015. doi: 10.18260/p.23835.

[17] Weidong Li, Amelia Lee, Melinda Solmon, "The role of perceptions of task difficulty in relation to self-perceptions of ability, intrinsic value, attainment value, and performance." Nov. 2023. Accessed: Dec. 20, 2024. [Online]. Available: https://journals.sagepub.com/doi/10.1177/1356336X07081797

[18] R. F. Kizilcec et al., "Scaling up behavioral science interventions in online education," Jun. 15, 2020, National Academy of Sciences. doi: 10.1073/pnas.1921417117.

[19] D. Oyserman, K. Elmore, S. Novin, O. Fisher, and G. C. Smith, "Guiding People to Interpret Their Experienced Difficulty as Importance Highlights Their Academic Possibilities and Improves Their Academic Performance," May 25, 2018, Frontiers Media. doi: 10.3389/fpsyg.2018.00781.

[20] D. Shoemaker, D. Davidson, and A. Conklin, "Toward a Discipline of Cyber Security: Some Parallels with the Development of Software Engineering Education," Dec. 02, 2017, Taylor & Francis. doi: 10.1080/07366981.2017.1404867.

[21] M. Bishop et al., "Cybersecurity Curricular Guidelines," in IFIP advances in information and communication technology, Springer Science+Business Media, 2017, p. 3. doi: 10.1007/978-3-319-58553-6_1.

[22] R. S. Baker, U. Boser, and E. L. Snow, "Learning engineering: A view on where the field is at, where it's going, and the research needed.," Mar. 31, 2022, American Psychological Association. doi: 10.1037/tmb0000058.

[23] T. Goodman and A.-I. Radu, "Learn-Apply-Reinforce/Share Learning: Hackathons and CTFs as General Pedagogic Tools in Higher Education, and Their Applicability to Distance Learning," Jan. 01, 2020, RELX Group (Netherlands). doi: 10.2139/ssrn.3637823.

[24] O. Chen, F. Paas, and J. Sweller, "A Cognitive Load Theory Approach to Defining and Measuring Task Complexity Through Element Interactivity," Jun. 01, 2023, Springer Science+Business Media. doi: 10.1007/s10648-023-09782-w.

AUTHORS

Khoo Li Jing is an academic in University of Wollongong Malaysia. His research interests are in game-based learning, andcybersecurity skill development. He is completing his Ph.D. in Game-Based Learning at Sultan Idris Education University, Malaysia. He completed his M.Sc. in Computer Network Security from Liverpool John Moores University, U.K., and his Bachelor in Information Systems from Tunku Abdul Rahman University of Management and Technology, Malaysia.

Maizatul Hayati Mohamad Yatim is an associate professor of Human-Computer Interaction in Computing Department, at Sultan Idris Education University, Malaysia. Her research interests are specifically on game design and development, game usability, and game-based learning. She received her Ph.D. in Computer Science from Otto-von-Guericke University of Magdeburg, Germany, her M.Sc. in Information Technology, and her Bachelor in Information Technology both from Northern University of Malaysia.

Ts. Dr. Wong Yoke Seng is the Deputy Director (Data & Strategic Planning), of the Research Management Centre in Universiti Perguruan Sultan Idris. His specialisation is in Game-based Learning. He received a B.S degree in Information System Engineering from Campbell University and M.S.C in Computer Game Technology from Liverpool John Moores University, UK. He has been teaching game design and game programming related subjects for over 20 years and actively involved in game related research projects. His current research involves using computer game as learning tool for learning object-oriented programming in tertiary level and his current interests are gamification, game design, data structures & algorithms and object oriented system analysis and design. Malaysia