Journal of Human Centered Technology

https://www.humentech.utm.my E-ISSN: 2821-3467

Research on Capture the Flag Exercises for Cybersecurity Skill Training Among Malaysian Undergraduates

Khoo Li Jing[1,2], Maizatul Hayati Mohamad Yatim[1], Wong Yoke Seng[1*]

[1]Faculty of Computing and Meta-Technology, Sultan Idris Education University, Tanjong Malim, 35900, Malaysia
[2]School of Computing and Creative Media, University of Wollongong Malaysia, Shah Alam, Selangor, 40150, Malaysia

*Corresponding Author yswong@meta.upsi.edu.my

Cite: https://doi.org/10.11113/humentech.v4n1.87 Research Article

Abstract:
Cybersecurity education is crucial for addressing the growing skills gap in industries, with Capture the Flag (CTF) exercises emerging as a promising gamified approach for engaging and training students in cybersecurity skills. This study introduces SKRCTF, an integrated framework that adapts CTF principles for Malaysian undergraduate cybersecurity education. Through a systematic integration of gamification elements and pedagogical principles, SKRCTF was designed to cater to the specific needs and challenges of Malaysian undergraduates in cybersecurity skill development. The framework's effectiveness was evaluated through a quasi-experimental study involving two Malaysian universities, using pre-test and post-test assessments. While initial results showed limited improvement in overall performance, the second iteration with enhanced scaffolding demonstrated significant progress in specific areas such as operating system threats and cryptography pattern recognition. These findings, though partially negative, provide valuable insights into the prerequisites and conditions necessary for effective CTF implementation in Malaysian higher education. The study contributes to the understanding of how gamified cybersecurity training should be adapted for different educational contexts, particularly highlighting the importance of fundamental computing knowledge and structured support systems. The SKRCTF framework and its implementation findings offer a foundation for developing more effective cybersecurity training programs tailored to Malaysian undergraduate education.

Keywords: Cybersecurity; Capture the Flag; Skill training; Undergraduates; Malaysia

1. INTRODUCTION

Cybersecurity skills are vital in the contemporary digital landscape, yet the industry confronts a significant skills gap. Capture the Flag (CTF) exercises, which replicate real-world cybersecurity challenges, have emerged as a promising approach to address this gap through hands-on learning. While CTF has been widely adopted in security conferences and competitions globally, its efficacy as a formal educational tool, particularly in developing countries like Malaysia, warrants further investigation (1). Nonetheless, most CTF events have been conducted in informal settings. Integrating CTF as a formal skill training method among Malaysian undergraduates has been limited in both study and implementation. This research aimed to explore the effects of CTF exercises as a skill training approach for learning cybersecurity among Malaysian undergraduates. Two universities were selected, where computing students practiced cybersecurity skills for the first time using a customized CTF platform, SKRCTF. The study introduces the context of CTF in cybersecurity skill development and its application in Malaysia, the theoretical framework of SKRCTF, and the methodology used to evaluate the effectiveness of CTF as a skill training method. The findings revealed no significant improvement in the cybersecurity skills of Malaysian undergraduates who participated in CTF exercises. The factors contributing to these results were discussed, suggesting that cybersecurity skills development requires learners with strong fundamentals in programming, networking, databases, and operating systems.

While CTF exercises have yielded positive outcomes in Western and some Asian nations by integrating them into cybersecurity education programs (2), the implementation and effectiveness of such gamified simulations may present distinct challenges and opportunities in the context of Malaysian higher education that merit thorough investigation. These CTF activities provide participants with hands-on experience in domains such as cryptography, reverse engineering, and web security. The Malaysian context offers an interesting case study for several reasons. Unlike many Western institutions where CTF is commonly used, Malaysian universities typically introduce computer science fundamentals at the tertiary level, potentially affecting how students engage with CTF exercises. Additionally, the integration of CTF into formal educational frameworks in Malaysia has been limited, with most cybersecurity competitions occurring in informal settings. To address these gaps and understand the potential of CTF as an educational tool in the Malaysian context, this research investigates three key questions:

Received 13 August 2024; Accepted 02 November 2024
Available online 06 February 2025

i. Is there a statistically significant difference in students' performance in acquiring fundamental cybersecurity concepts before and after learning through a CTF game?
ii. Is there a statistically significant difference in students' performance in acquiring types of cybersecurity threats before and after learning through a CTF game?
iii: Is there a statistically significant difference in students' performance in acquiring cryptography concepts before and after learning through a CTF game?

This study employed a customized CTF platform, SKRCTF, tailored to the needs of Malaysian undergraduates. Through a quasi-experimental design involving two universities, the researchers evaluated the impact of CTF exercises on students' acquisition of cybersecurity skills and engagement. The findings of this research contribute to our understanding of how CTF can be effectively integrated into diverse educational contexts and provide insights for developing more impactful cybersecurity training programs in Malaysia.

2. THE ROLE OF CTF IN CYBERSECURITY SKILL DEVELOPMENT

Capture the Flag was originally developed as a competitive game in the context of information security (3). There are 2 formats of CTF: Jeopardy and attack and defense (4). In the United States, CTF has been widely adopted in security conferences and competitions, where participants race against the clock to find hidden flags or exploit vulnerable systems (4). Defcon and The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge are among the competitions that have popularized the concept of CTFs (5, 6). A typical CTF activity involves a set of security challenges that require participants to demonstrate knowledge in areas such as cryptography, reverse engineering, binary exploitation, web security, and digital forensics (7). Team members in CTF should consist of various subject matter experts to obtain the most flags or score the highest to win the competition. Cybersecurity domains cover a wide range of realms and require different skill sets.

Beyond competitions, security researchers have also explored the use of CTF as an educational tool for teaching and training cybersecurity skills (8). Research was conducted among tertiary-level institutions and even at the high school level. PicoCTF and VolgaCTF are examples of CTF platforms designed specifically for educational purposes (9) However, most research on the effectiveness in skill development focused on Western countries, lacks study in the context of developing countries such as Malaysian undergraduates (4, 10). Recent studies in Southeast Asia have shown varying approaches to CTF implementation. For example, Vietnamese universities successfully integrated CTF with existing cybersecurity curricula by emphasizing cultural learning preference (11). Similarly, Indonesian researchers demonstrated how regional tech infrastructure influences CTF effectiveness (12). These regional studies provide valuable context for understanding CTF implementation challenges in Malaysia.

2.1 Understanding The Structure and Mechanics of CTF

Regarding simulations and Game-based Learning (GBL), CTF can be considered a gamified approach that mimics realistic security challenges to engage learners and enhance their problem-solving skills in a safe environment (13). A standard CTF consists of the elements of the GBL framework: Learning objectives, game mechanics, feedback and reflection, learner engagement and scaffolding, assessment, and progression (14–17). Storytelling or narratives are rarely included in CTFs due to the nature of the skill training approach. Participants were found skipping the story mode and jumping directly into the standard format once they understood the competition format (18).

A standard CTF duration lasts from hours to days, with challenges ranging in difficulty levels to cater to participants with different expertise. Within the CTF environment, participants are required to demonstrate their understanding and application of cybersecurity concepts and techniques (19). Game mechanics require participants to be aware of time constraints, team collaboration, information gathering, vulnerability discovery, and exploitation. The organizer will prepare a set of challenges with various difficult levels, releasing them at different times in the competition. Hints are given out if no participant can solve the challenge.

A CTF structure consists of a scoring system and leader board, challenge management, user and team management, regulation control, and communication tools. During the competition, the organizer is responsible for maintaining the game platform, releasing challenges, monitoring participants' activities, and providing technical support. Participants can obtain immediate feedback on their performance via the scoring system and leaderboard (20). Conversely, they will receive an immediate warning if they perform malicious activity such as attacking the scoring system or sharing flags.

2.2 Impact of CTF on Undergraduate Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) Framework constructed a common structure that describes cybersecurity work and the knowledge, and skills needed to complete that work based on job roles. Educational institutions are still finding the most effective method to enhance learners' competency. Prior research concluded that most cybersecurity education requires practical skills besides theoretical concepts. CTF is considered a hands-on approach that can potentially bridge the gap between theory and practice (3). Based on the reviewed literature, there are several benefits of using CTF in cybersecurity education. (13).

Mirkovic and Peterson proposed the "Class-CTF" model, where CTF is adapted as a classroom-based learning activity, with challenges tied to learning objectives and integrated into the curriculum over a longer period (20). The study's outcome showed that students could learn cybersecurity concepts and skills by integrating CTFs in the classroom, achieving the intended learning outcomes (21). Further research was done by adopting a similar approach, showing similar outcomes (21, 22). Recent developments in Southeast Asian cybersecurity education show emerging trends in CTF adoption. A comprehensive study of Thai universities revealed that successful CTF implementation strongly correlates with existing

information technology (IT) infrastructure and instructor expertise (23). Singapore's experience demonstrates how cultural factors influence student engagement with gamified learning platforms (24). These regional insights help contextualize Malaysia's unique challenges and opportunities in CTF implementation.

It has less significant findings on using a similar environment in Malaysia. With the similar wording of “hack” in the name, Hackathons in Malaysia are primarily focused on developing applications and pitching business ideas rather than cybersecurity, indicating a gap in the use of gamified learning for cybersecurity skills development. Considering the differences in educational systems and approaches to problem-solving between Western and Asian countries, the effectiveness of CTF in developing cybersecurity skills among Malaysian undergraduates remains inconclusive. Some participants may have better access to training materials, tools, or mentorship.

General Malaysian students are exposed to a formal computer science curriculum at tertiary level education. The curriculum typically covers programming, databases, networking, and operating systems topics as core subjects (25). Skill-based cybersecurity subjects may not be suitable to be introduced in the early years of the undergraduate program. Based on the previous findings by various researchers, this research is conducted to study the suitability of CTF in Malaysia context.

2.3 Theoretical Framework

This research is grounded in Kolb’s Experiential Learning theory, which proposes that learning occurs through a cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation (20). CTF are exposed to real-world cybersecurity challenges, enabling them to apply their theoretical knowledge to solve practical problems. Participants engage directly with CTF challenges to obtain the concrete experiment, then reflect on their performance after submitting flags to the server. Participants then form theories and strategize to tackle the wrong submission or more complex challenges to exhibit that they can apply their new understanding to subsequent challenges.

To ensure the integration of GBL is pedagogically sound and technology feasible, Technological Pedagogical Content Knowledge (TPACK) is adopted (26). Our framework selection and adaptation build upon recent research that validates the effectiveness of gamification frameworks in technical education within Southeast Asian contexts (26). This work demonstrates that while Western frameworks provide valuable foundations, their successful implementation in Asian educational settings requires careful consideration of local learning cultures and educational practices. Educators may have been trained to conduct specific cybersecurity skills but tasked to collaborate with CTF administrators to implement GBL strategies into the CTF platform to enhance learning experience. Moreover, the cybersecurity challenges are aligned and represented through the CTF challenges at the participants’ learning capacity. The core principles of gamification remain relevant across educational levels, though the implementation differs. In our adaptation, we focused particularly on gamification elements in CTF design while adjusting the complexity and scaffolding approaches to match undergraduate-level learning needs in e-learning experience. This framework consists of understanding the target audience, structuring the experience, identifying resources, applying gaming elements, and implementing monitoring mechanisms. The integrated framework shown in Figure 1 provides a comprehensive view of designing and developing CTF as a pedagogical tool for cybersecurity education. A customized CTF, namely SKRCTF was designed and developed based on the integrated framework and was piloted with a cohort of undergraduates taking a cybersecurity module at two local universities.

2.3.1 Gamification elements in CTF design

This research integrates two key theoretical foundations: Kolb's Experiential Learning theory and gamification principles in educational design. While CTF inherently contains gaming elements, a structured gamification framework ensures pedagogically sound implementation. CTF naturally embodies core gamification principles that support cybersecurity learning:

1. Clear Goals and Rules. Objectives and rules of the CTF are explicitly stated, allowing participants to understand the gameplay and align their actions accordingly. Structured point systems are based on challenge difficulty and flag submission provide clear performance indicators. Ethical boundaries and competition regulations are also pre-defined.
2. Progressive Difficulty Levels CTF. Challenges are set at different difficulty levels, allowing participants to start with easier tasks, build confidence, and gradually progress towards more complex challenges. Participants pace themselves in the through difficulty tiers in the “CTF world map”.
3. Immediate Feedback system. Real-time submission verification is conducted in a CTF session and performance tracking via leaderboard allows participants to get immediate feedback on their progress. Some CTF challenges provide dynamic scoring updates to encourage participants to be more innovative in their problem-solving approaches.
4. Competitive and Collaborative Elements. CTF is inherently competitive, with participants competing for the highest scores. Participants enjoy the peer learning opportunities in a team setting to collectively solve challenges. CTF may also incorporate collaborative elements, where teams cooperate to achieve common goals.

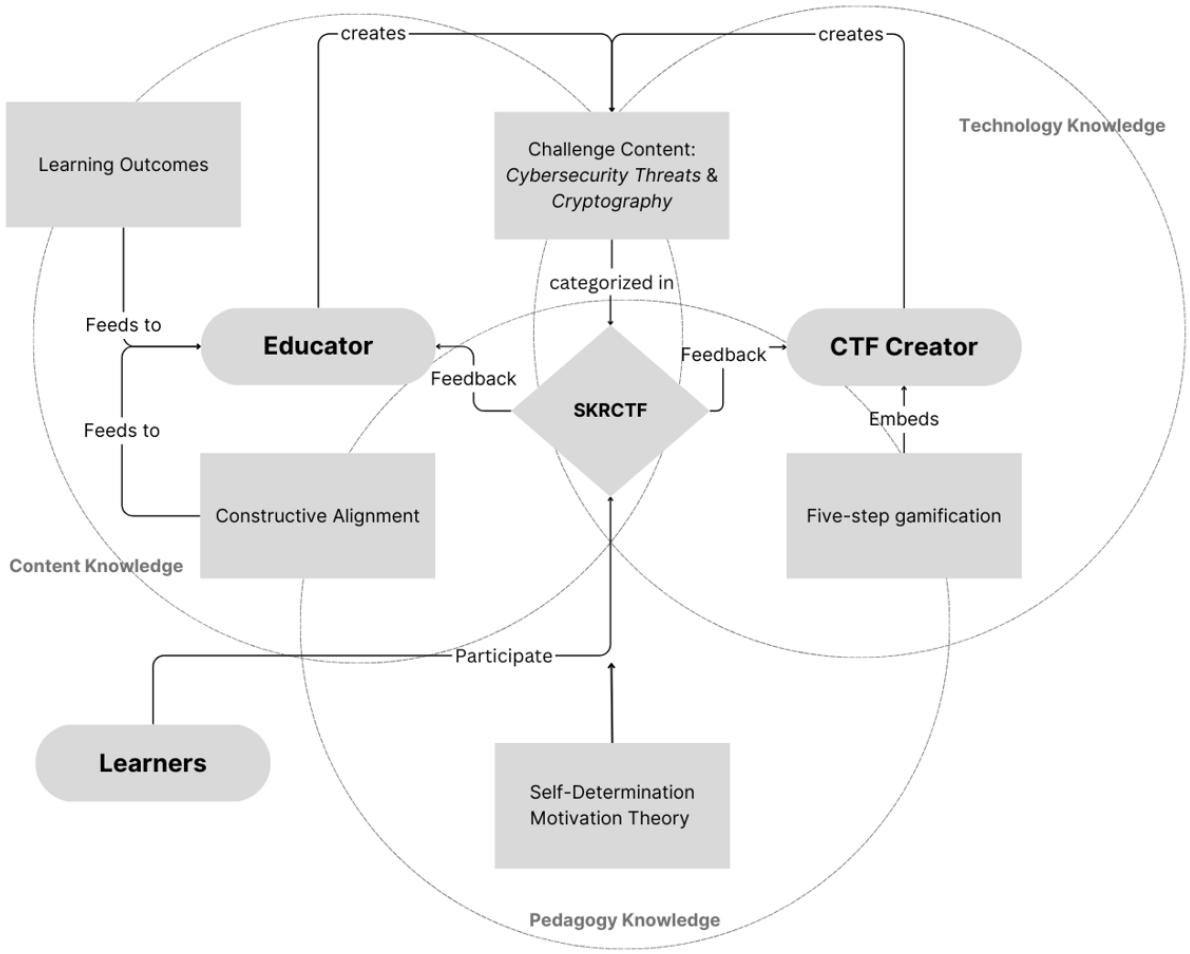

Figure 1. Proposed framework in preparing SKRCTF as a cybersecurity skill training game.

The gamification elements incorporated align with the key game design principles identified by Deterding et al. for non-game applications (27). Recent validation studies support the adaptation of gamification elements for technical education in Southeast Asian contexts. This research confirms that core gamification principles remain effective when properly contextualized for local educational environments (28). These elements are particularly well-suited for supporting cybersecurity education, as they create safe environments for hands-on experimentation and foster ongoing skill development among learners.

2.3.2 Integration of Learning and Gamification Frameworks

SKRCTF was guided by the TPACK framework. The game's Pedagogical Content Knowledge (PCK) was validated by four experienced academicians, and its Technology Content Knowledge (TCK) was assessed by 2 cybersecurity professionals. Lastly, the Technology Pedagogical Knowledge (TPK) was validated by a Game-Based Learning academician. The SKRCTF framework combines Kolb's Experiential Learning theory with structured gamification implementation through five key phases (29):

1. Understanding the target audience and learning objectives. This involves identifying the key characteristics, needs, and preferences of the participants to ensure the SKRCTF challenges align with their skill levels and learning goals.
2. Structuring the experience. This entails planning the game format, challenge levels, scoring system, and other game mechanics to create an engaging and meaningful learning environment.
3. Identifying resources. This involves the necessary resources, such as hardware, software, challenge scenarios, and facilitator support, to enable smooth implementation of SKRCTF.
4. Applying gaming elements. This step involves the actual design and development of the SKRCTF platform, incorporating game elements like points, leaderboards, peer learning and feedback systems to enhance the participant's engagement and learning experience.
5. Continuous Monitoring. This includes evaluating the CTF to gather feedback, identify areas for improvement, and make iterative changes to enhance the learning experience.

3. METHODS

This research employs a quantitative method with a non-equivalent control group pre-post experiment design. The independent variable was set to the design of SKRCTF while the dependent variable was set to the learner's competency level. Population and sampling were consisted of two groups of cybersecurity undergraduate students, one control group and one experimental group, with a total of 71 participants. The control group received the regular cybersecurity curriculum without SKRCTF intervention. The experimental group, on the other hand, participated in the customized CTF sessions in addition to the regular curriculum. Both groups were given the same 15-multiple-choice questions in the pre-test and post-test. The data collected from the pre-and post-tests were analyzed using Mann-Whitney-U and McNemar Test. The experiment spans one semester, with SKRCTF sessions been integrated and conducted over 10 weeks. Two universities were selected, and the students were randomly assigned to the control and experiment groups. All participants underwent the same pre-test to minimize potential bias (13, 21).

The findings showed no statistically significant differences in the performance of the experimental group who participated in the SKRCTF sessions compared to the control group who did not. The possible reasons were that the students may not have sufficient prior knowledge and skills to effectively participate in the SKRCTF challenges and the lack of scaffolding and feedback mechanisms in the SKRCTF design. The pre and post-test questions were revised, and a second experiment was conducted.

4. RESULTS AND DISCUSSION

The experiment was conducted during Malaysia's Movement Control Order (MCO) when students were attending online classes. The inconsistency and incomplete submission led to a high discard rate of data samples. The sample size is shown in Table 1. University B has a larger population compared to University A.

Table 1: Source and quantity of samples.

University	Group	Size
A	Learn cybersecurity topics the conventional methods	11
	Learn cybersecurity topics with SKRCTF	13
B	Learn cybersecurity topics the conventional methods	7
	Learn cybersecurity topics with SKRCTF	40

Shapiro Wilk test exhibited that the data is not normally distributed ($W(71) = 0.929$, $p<0.01$), hence non-parametric tests were performed. The overall scores of the control and experimental groups were compared using the Mann-Whitney U test. The results showed no statistically significant difference ($p=0.347$, $Z=-.940$) in the performance of the control and experimental groups. Further tests were conducted to find the factors that lead to similar performance levels between the two groups. Table 2 shows that the two groups found no significant difference in the pre-test. Both groups had the same performance level before the intervention. However, the post-tests showed a similar trend of insignificant difference between the control and experimental groups. The Mann-Whitney U test confirms that SKRCTF intervention did not lead to a statistically significant improvement in the overall performance scores compared to the regular curriculum ($p = 0.403$, $Z = -.837$). The overall mean for the control group increased but the experiment group suffered a decrease after the post-tests. The control group scored an average of 1.78 on the pre-test and 2.17 on the post-test while the experimental group obtained 2.66 on the pre-test and 2.51 on the post-test.

Table 2: Test item 5 on assessing operating system threats.

Pre-test 5: How do you interpret the situation below (CS) & Post-test 5: How do you interpret the situation below (CS)

Pre-test 5: How do you interpret the situation below (CS)	Post-test 5: How do you interpret the situation below (CS)	
	Incorrect	Correct
Incorrect	27	11
Correct	1	1

Further tests on each university were conducted to investigate the factors that contributed to the decline in performance. The overall mean for University A's control group ($N=11$) and experiment group ($N=13$) increased after the post-tests. The control group scored an average of 2.00 on the pre-test and 2.45 on the post-test while the experimental group obtained 3.23 on the pre-test and 3.38 on the post-test. However, the improvement between the two groups failed to display a significant difference ($p=0.915$, $Z=-1.55$).

University B exhibited a different trend. The overall mean for the control group increased but the experiment group suffered a decrease after the post-tests. The control group scored an average of 1.43 on the pre-test and 1.71 on the post-test while the experimental group obtained 2.47 on the pre-test and 2.23 on the post-test. Further tests on each university were conducted to investigate the factors that contributed to the decline in performance.

Additionally, the McNemar test was performed to examine any significant changes within the universities. 11 participants from University B had shown improvement in recognizing Operating System threats (Test item 5) even though there were still 27 participants who got wrong in the post-test. In recognizing file encoding (Test item 11), university B students showed a significant regression between the scores. 0 participants successfully recognized a hidden code pattern in the post-test compared to 13 in the pre-test.

Table 3: Test item 11 on assessing file encoding.

Pre-test 11: What do you analyze from the screen below? (CP) & Post-test 11: What does the highlighted text below mean in a file? (CP)

Pew-test 11: What do you analyze from the screen below? (CP)	Post-test 11: What does the highlighted text below mean in a file? (CP)	
	Incorrect	Correct
Incorrect	26	1
Correct	13	0

The negative results from our first experiment, while not achieving the expected improvement in cybersecurity skills, provide valuable insights into the complexities of implementing CTF-based training in Malaysian higher education. These findings are particularly significant as they highlight critical factors that weren't previously well-documented in the literature for Malaysia:

1. Online Learning Environment Impact. The study's timing during Malaysia's Movement Control Order revealed limitations of online-only CTF implementation. The high discard rate and inconsistent submission suggest that virtual CTF environments without proper support may be insufficient for skill development. This contrasts with Western studies reporting success with online CTF, indicating potential cultural or infrastructure differences to consider.
2. Prerequisites and Scaffolding. A more structured and comprehensive approach to prerequisite skill development, such as building a strong foundation in computing fundamentals like programming logic, cryptographic algorithms, operating systems, networking, and databases, might be necessary to enable students to effectively participate in and benefit from CTF challenges.

The findings from the second experiment showed that the experimental group who participated in the revised CTF sessions still failed to perform significantly better in the post-test compared to the control group, even showing slight improvement in 1 topic. Without the physical presence of the facilitator to guide the students on the SKRCTF learning experience, the students may have struggled to navigate the SKRCTF challenges independently. Besides providing hints about the SKRCTF challenges, scaffolding from the instructors on the thought process and technical knowledge to solve the problems could be crucial in enhancing the effectiveness of CTF-based learning (30–33).

A second experiment was conducted in May 2022, with a new batch of 33 participants from University A splitting into 17 in the control group and 16 in the experimental group receiving the revised SKRCTF intervention. Similar 15-multiple-choice questions were provided in the pre-and post-tests. The mean score for all the pre-test participants was 6.09 out of 15 with a standard deviation of 2.919. In the post-test, the control group scored a mean of 4.82 with a standard deviation of 2.157, while the experimental group scored a mean of 8.56 with a standard deviation of 3.032. The Mann-Whitney U test revealed a statistically significant difference (p<0.001) between the post-test scores of the control and experimental groups, with the experimental group outperforming the control group.

In tackling research question 2, McNemar Test was conducted to analyze each test item. 2 out of 8 test items showed a significant difference, namely test item 5 (p=0.031) and test item 12 (p=0.008). The cybersecurity threat topics included Operating System commands and Shellcode. This indicates that the revised SKRCTF intervention has improved the students' ability to recognize specific cybersecurity threats compared to the control group receiving the standard curriculum.

In analyzing research question 3 on recognizing cryptography patterns, test item 9 showed a significant difference, with 5 participants from the experimental group improving from the pre-test and 3 participants maintaining the correct answer in both the pre-test and post-test for calculating public key cryptography.

Only 3 out of 15 test items exhibited a significant improvement in building cybersecurity skills after the revised SKRCTF intervention. Perhaps, technical cybersecurity topics were difficult to conduct at the beginner level. Learners are required to equip themselves with computing fundamentals such as programming logic, cryptographic algorithms, operating systems, networking, and databases before applying them in a CTF scenario. On a positive note, both experiments revealed that participants can recognize system administration-related topics in both experiments after playing SKRCTF. Furthermore, learners from the second experiment showed significant improvement in recognizing types of malicious code used in specific situations.

5. CONCLUSION

In answering the first research question, the initial experiment did not find a significant difference in the overall performance between the control and experimental groups after the SKRCTF intervention. The revised SKRCTF intervention in the second experiment, however, showed a significant improvement in the overall performance of the experimental group compared to the control group. However, achieving 3 out of 15 test items with significant differences still suggests that CTF is not sufficient as a standalone learning activity. From the second and third research questions, it is concluded that learners

need to obtain a solid foundation of computing concepts before diving into cybersecurity. The areas include programming logic, computer networking, database and operating systems. Gap exists within specific areas of cybersecurity skills such as cryptography, malware, and intrusion detection. The contrasting results between the 2 universities can also be attributed to the different baseline knowledge of the participants on cybersecurity. Different institutional approaches to fundamental computing education and access to resources could be vital factors.

This initial experiment has contributed significantly to our understanding of CTF implementation in several ways:

1. Prerequisite Knowledge Framework: Our findings help establish a clearer framework for the prerequisites needed before implementing CTF training. The initial experiment's results, while not showing improvement, helped identify specific knowledge gaps that need to be addressed in curriculum design.
2. Implementation Guidelines: The contrast between our first and second experiments highlights valuable insights for future CTF implementations. These include the need for a balanced approach incorporating both online and face-to-face interactions, the importance of structured scaffolding, the role of instructor guidance in the learning process, and the value of progressive difficulty levels in challenge design.
3. Contextual Considerations: This study underscores the need to account for local educational contexts when adopting Western-developed teaching approaches. The findings suggest that successful implementation of CTF in Malaysian universities may necessitate:
    - Tailored approaches to accommodate diverse educational backgrounds
    - Supplementary support structures beyond those typically emphasized in Western research
    - Heightened focus on cultivating fundamental skills
    - Integration with existing curricular frameworks

These findings, while not aligning with our initial hypotheses, offer critical insights to guide future research and implementation of cybersecurity training in analogous contexts. They suggest that effective deployment of CTF exercises necessitates a more nuanced and structured approach than what has been previously recommended in the literature, particularly in developing countries where the frameworks of computing education may diverge from Western models. The results of this study indicate that SKRCTF as a skill training approach may not be as effective as expected in improving the cybersecurity competency of Malaysian undergraduate students in the short term, especially when conducted in an online environment without the necessary scaffolding from instructors. However, there are opportunities to enhance SKRCTF design and implementation through learner-centric and scaffolding approaches. The SKRCTF tasks should be tailored to the learners' existing knowledge and skills to ensure they can progress through the challenges effectively and meaningfully. To yield a positive outcome, facilitators must pace the participants with proper exposure to various difficulty levels in gaining cybersecurity knowledge and skills through SKRCTF or related CTF games. Future research on using CTF as a learning tool to gain cybersecurity knowledge and skills should be tailored to the specific skill levels and learning needs of the undergraduate population could enhance the effectiveness of this training method (34). Peer learning and assessment could be a valuable addition to the CTF-based training. Incorporating peer-to-peer feedback and evaluation of the CTF challenges and performance can help students learn from each other, identify areas for improvement, and foster a collaborative learning environment (35). By addressing these factors, CTF-based learning has the potential to become a more valuable and impactful tool for developing cybersecurity competencies among undergraduates.

AUTHORSHIP CONTRIBUTION STATEMENT

Khoo Li Jing: data curation, investigation, resources, software, writing – original draft, visualization; Maizatul Hayati Mohamad Yatim: conceptualization, funding acquisition, methodology, supervision; Wong Yoke Seng: formal analysis, project administration, validation, writing – review & editing

DATA AVAILABILITY

Data are available within the article and/or its supplementary materials.

DECLARATION OF COMPETING INTEREST

No conflict of interest.

ACKNOWLEDGMENT

No acknowledgment to declare.

REFERENCES

(1) Chang SY, Yoon K, Wuthier S, Zhang K. Capture the flag for team construction in cybersecurity. arXiv. 2022. https://doi.org/10.48550/arXiv.2206.08971.
(2) Liu DYW, Leung ACY, Au MH, Luo X, Chiu PHP, Im SWT, Lam WMW. Virtual laboratory: Facilitating teaching and learning in cybersecurity for students with diverse disciplines. 2019 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE). 2019; 1–6. https://doi.org/10.1109/TALE48000.2019.9225863.

(3) Vykopal J, Švábenský V, Chang EC. Benefits and pitfalls of using capture the flag games in university courses. Proceedings of the 51st ACM Technical Symposium on Computer Science Education. 2020;752–758. https://doi.org/10.1145/3328778.3366893.
(4) Horcher AM. Shall we play a game? Building capture the flag games for non-traditional players. 2020 Research on Equity and Sustained Participation in Engineering, Computing, and Technology (RESPECT). 2020;1–2. https://doi.org/10.1109/RESPECT49803.2020.9272410.
(5) Cyber Grand Challenge. MIT Lincoln Laboratory [Internet]. Mit.edu. 2016 [cited 2024 Aug 12]. Available from: https://www.ll.mit.edu/research-and-development/cyber-security-and-information-sciences/cyber-grand-challenge.
(6) Darpa.mil. [Internet]. 2021. [cited 2024 Aug 12]. Available from: https://www.darpa.mil/program/cyber-grand-challenge
(7) Zhang XY, Liu B, Gong X, Song Z. State-of-the-art: Security competition in talent education. Lect Notes Comput Sci. 2017.
(8) Pusey P, Tobey D, Soule R. An Argument for game balance: Improving student engagement by matching difficulty level with learner readiness [Internet]. Usenix.org. 2014 [cited 2024 Aug 12]. Available from: https://www.usenix.org/conference/3gse14/summit-program/presentation/pusey.
(9) Seda P, Vykopal J, Svabensky V, Celeda P. Reinforcing cybersecurity hands-on training with adaptive learning. 2021 IEEE Frontiers in Education Conference (FIE). 2022. https://doi.org/10.1109/FIE49875.2021.9637252.
(10) Timmins J, Knight S, Lachine B. Offensive cyber security trainer for platform management systems. 2021 IEEE International Systems Conference (SysCon). 2021. https://doi.org/10.1109/SysCon48628.2021.9447060.
(11) Nguyen TA, Pham H. A design theory-based gamification approach for information security training. IEEE; 2020;1–4. https://doi.org/10.1109/RIVF48685.2020.9140730.
(12) Kartasasmita DG, Timur FGC, Reksoprodjo AHS. Enhancing competency of cybersecurity through implementation of the “CAPTURE THE FLAG” on college in Indonesia. Int J Humanities Educ Soc Sci. 2023; 3(2). https://doi.org/10.55227/ijhess.v3i2.710.
(13) Leune K, Petrilli SJ. Using capture-the-flag to enhance the effectiveness of cybersecurity education. Proceedings of the 18th Annual Conference on Information Technology Education. 2017.
(14) Jabbar AIA, Felicia P. Towards a conceptual framework of GBL design for engagement and learning of curriculum-based content. Int J Game-Based Learn. 2016; 6(4):87–108.
(15) Gáliková M, Valdemar Švábenský, Vykopal J. Toward guidelines for designing cybersecurity serious games. 2021.
(16) Plass JL, Homer BD, Kinzer CK. Foundations of game-based learning. Educ Psychol. 2015; 50(4):258–83.
(17) Zhao N, Xiong M, Zhongguancun B, Cn X, Zhang, Terwilliger M. Issues in information systems proposing a framework of game-based learning and assessment systems. 2021; 22(4):193–207.
(18) Chapman P, Burket J, Brumley D. PicoCTF: A game-based computer security competition for high school students [Internet]. www.usenix.org. 2014 [cited 2024 Aug 12]. Available from: https://www.usenix.org/conference/3gse14/summit-program/presentation/chapman.
(19) Antonioli D, Reza H, Sridhar G, Martín A, Nils O, Tippenhauer O. Gamifying education and research on ICS security: Design, implementation and results of S3. Cryptography and Security. https://doi.org/10.48550/arXiv.1702.03067.
(20) Mirkovic J, Peterson PAH. Class capture-the-flag exercises [Internet]. www.usenix.org. 2014. [cited 2024 Aug 12]. Available from: https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic.
(21) Goodman T, Radu AI. Learn-apply-reinforce/share learning: Hackathons and CTFs as general pedagogic tools in higher education, and their applicability to distance learning. SSRN Elect J. 2020. http://dx.doi.org/10.2139/ssrn.3637823.
(22) Karagiannis S, Magkos E. Adapting CTF challenges into virtual cybersecurity learning environments. Inform Comp Secur. 2020; 29(1):105–32. https://doi.org/10.1108/ics-04-2019-0050.
(23) Sookhanaphibarn K, Choensawat W. Educational games for cybersecurity awareness. 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE). 2020; 424–428. https://doi.org/10.1109/GCCE50665.2020.9291723.
(24) Tan KH, Ouh EL. Lessons learnt conducting capture the flag cybersecurity competition during COVID-19. 2021 IEEE Frontiers in Education Conference (FIE). 2021; 1–9. https://doi.org/10.1109/FIE49875.2021.9637404.
(25) Bin Ibrahim AD, Ashrofie Hanafi AH, Rokman H, Ahmad Zawawi MN, Ibrahim ZA, Rahim FA. Comparative analysis on student’s interest in cyber security among secondary school students using CTF platform. IEEE Xplore. 2020; 73–77. https://doi.org/10.1109/ICIMU49871.2020.9243561.
(26) Nurhidayah L, Suyanto S. Integrated of technological pedagogical and content knowledge (TPACK) for pre-service science teachers: Literature review. Netherland: Atlantis Press; 2021. https://www.atlantis-press.com/proceedings/isse-20/125954815
(27) Khoo LJ, Maizatul HMY, Wong YS. A preliminary concept on cybersecurity skill training framework for a capture-the-flag game using 5-step gamification approach. Int J Multimedia Appl. 2024; 16. https://doi.org/10.5121/ijma.2024.16402.
(28) Kamalodeen VJ, Ramsawak-Jodha N, Figaro-Henry S, Jaggernauth SJ, Dedovets Z. Designing gamification for geometry in elementary schools: insights from the designers. Smart Learn Environ. 2021; 8(1). https://doi.org/10.1186/s40561-021-00181-8.
(29) Deterding S, Dixon D, Khaled R, Nacke LE. From game design elements to gamefulness: defining “gamification.” ACM. 2011; 9–15. https://doi.org/10.1145/2181037.2181040.
(30) Lai L-C, Hu Y-C, Wang Y-Te, Chen J-L. The study of constructivism oriented web-based learning on the performance of technological college students. [Internet]. 2010 [cited 2024 Aug 12]; Available from: https://ieeexplore.ieee.org/document/5564714/
(31) Afifah WA. Developing culture-based english instructional materials for grade VII of junior high school students. English Lang Teach Educ J. 2019; 1(2):76. https://doi.org/10.12928/eltej.v1i2.390.

(32) Loso MM. The information and communication technology (ICT) faculty relief project: An assignment algorithm for secondary schools' operations management [Internet]. Consortia Academia. 2022 [cited 2024 Aug 12]. Available from: https://consortiacademia.org/10-5861-ijrse-2022-204.
(33) Owston R, Wideman H, Ronda NS, Brown C. Computer game development as a literacy activity. Comp Educ. 2009; 53(3):977–89. https://doi.org/10.1016/j.compedu.2009.05.015.
(34) Szedlak D, M'manga A. Eliciting requirements for a student-focussed capture the flag. 2020 7th International Conference on Behavioural and Social Computing (BESC). 2020; 1–4. https://doi.org/10.1109/BESC51023.2020.9348329
(35) Goodman T, Radu AI. Learn-apply-reinforce/share learning: hackathons and CTFs as general pedagogic tools in higher education, and their applicability to distance learning. SSRN Elect J. 2020. http://dx.doi.org/10.2139/ssrn.3637823.