Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning

Tuan M. Tran*, Razvan Beuran, and Shinobu Hasegawa

***Abstract*—Present era of massive use of the internet has brought us enormous access to information and knowledge, yet has exposed us to such cybersecurity threats as personal information fraudulency and theft. Therefore, to safely and beneficially use cyberspace's information services, it is necessary and inevitable to raise awareness of cybersecurity. Aiming at building an environment to support cyberspace users in focusing and strengthening such awareness, we think that providing users with self-regulated learning courses about cybersecurity topics will be a practical approach. With that purpose in mind, in this paper, we introduce a framework for developing a gamification-based cybersecurity awareness course on the Moodle learning management system.**

***Index Terms*—Cybersecurity awareness, gamification, learning management system, self-regulated learning**

I. Introduction

Nowadays, cyberspace seems to be a typical doorway to approach data, information, and knowledge for most users, especially office employees and higher education students. Users of cyberspace, because of its ease of use and tremendous benefits, have lost awareness of cybersecurity.

According to a definition from the National Institute of Standard and Technology (NIST) of the U.S. Department of Commerce, cybersecurity is "*the ability to protect or defend the use of cyberspace from cyber attacks*" [1]. Cybersecurity is one of the most challenging yet exciting topics for students and practitioners in information science, software engineering, and information technology, as well as for ordinary users in everyday life. As internet-based services and applications have been growing rapidly and sophisticatedly into almost every societal corner, they benefit our daily-life activities. Unfortunately, they are also exploited for harmful purposes such as attacking users' privacy information and identity or stealing property virtually and physically [2].

Grounded in cybersecurity vulnerabilities and harmful exploitation is mainly users' unawareness of cybersecurity risks, which results in the users unconsciously opening such channels for cyber attacks such as password attacks, disclosure of private information, or running malicious software [2]. Target victims of such cybersecurity attacks are, most of the time, ordinary users who might range from office employees to college or university students, who use cyberspace for everyday life- and job-related activities such as searching materials for work or research, doing online shopping, sharing posts on social networks, installing software from online vendors. Unlike expert users who are students or practitioners of information science and who have knowledge and skills about cybersecurity and are aware of it, the ordinary users, because of lack of cybersecurity background, might not acknowledge how easy it is that they encounter such threats from their everyday activities such as checking emails, clicking internet links, and so forth on cyberspace. Given the above concerns, it is essential to provide users, especially the ordinary, with "*basic security concepts*" [2, p. 2] so that they build and strengthen their cybersecurity awareness in order to prevent cybersecurity threats from happening in the first place.

Cybersecurity varies in terms of bodies of knowledge, skills, and target audiences and learners. Therefore, understanding about cybersecurity stretches a wide range of degrees of competencies and applications [3]. Because the effectiveness of deep learning paths in a domain starts with awareness of such discipline, we propose, in this paper, a framework for developing a cybersecurity awareness course for ordinary users of cyberspace. The objectives of the course are:

- to awake learners' attention on security aspects which they encounter when using information services on cyberspace;
- to introduce appropriate responses to corresponding security risks; and
- to provide learners with practical cybersecurity scenarios.

As a proof of concept, this cybersecurity awareness course is designed for self-regulated learners in university or college settings in which the self-regulated learners have a certain maturity of self-education. The assessment of this awareness course will contribute insights for adjusting course topics, learning approaches, support mechanisms for self-regulated learning, which are necessary for designing such a course to outreach learners of a broader scale.

The main contributions of this paper are:

- A framework for building practical cybersecurity courses taking advantage of free learning management systems such as Moodle and free open sources of educational material.
- An approach to attract learners to courses and to retain their engagement so that they benefit from the courses regarding their improved knowledge as well as their way of learning.

To achieve those purposes, we structure the rest of the paper as the following. Starting with Section II, we present related work about the ideas of self-regulated learning, gamification, and mastery learning corresponding to how learners should learn, how to motivate learners, and the pattern of the course content, respectively. And then, in

Manuscript received February 25, 2022; revised April 11, 2022, accepted April 30, 2022.

The authors are with the Japan Advanced Institute of Science and Technology (JAIST), Ishikawa, Japan.

*Correspondence: tran.minh.tuan@jaist.ac.jp (T.M.T.)

doi: 10.18178/ijiet.2023.13.4.1859

Section III, we illustrate the framework for designing the course. After that, in Section IV, we briefly describe a concrete course developed by using the framework and implemented on Moodle. And finally, in Section V, we end the paper with conclusions and future works.

II. Related Work

A. Self-Regulated Learning and Learning Management System

Self-regulated learning (SRL) is a learning approach whereby learners actively set learning goals and objectives, monitor and control their learning progress, and reflect on their cognitive performance. SRL is indispensable in learning contexts such as online learning, distance learning, or e-learning where learners have no direct personal instructions or assistance. Although SRL is an inherent natural ability [4], the complexity and difficulty of knowledge sometimes prevent learners from self-regulating their learning. To self-regulate one's learning, one should maintain motivation, cognitive engagement, and metacognitive management, and gamification is a promising manner for achieving so.

Observing SRL, we might want to know from what factors SRL is made, how SRL operates, why a self-regulated learner learns effectively, and how a learner applies SRL into his or her own online learning context.

When learning, we apply our analytic and rational thoughts into objects that we learn to obtain knowledge, and we also contemplate our process of analysis of the object. There are two main processes involved in the understanding of knowledge: a cognitive process that absorbs knowledge and a metacognitive process that governs the cognitive process [5]. The more mature in SRL a learner gets, the more the learner is aware and in control of his or her cognitive and metacognitive process, and she/he is more proficient at learning.

Agreed by SRL models, an SRL process shares three common stages: planning a learning path; executing, monitoring and controlling the learning process; and assessing the effectiveness of the learning process [6]. A self-regulated learner starts a learning process with a stage of setting learning goals and objectives, and planning resources and activities applied into the learning journey. After planning, the learner continues the learning process by executing the learning plan toward the predefined goals. Simultaneously, she/he governs his or her learning by monitoring the effectiveness and efficiency of his or her learning and making adaptive changes of cognitive activities, time, learning environments, and external supports. Finally, when reaching end goals or time limit, the self-regulated learner reflects on his or her learning journey to reveal how well the learning process has been to the extent of, but not limited to, knowledge absorption, effectiveness, and efficiency of metacognitive and cognitive activities, and alternatives for better learning. The result of an SRL process is the growth of knowledge and the growth of SRL ability itself.

Looking at an SRL process, we see how active a learner can control his or her learning process over learning contents. Press it further. For learners to self-regulate their learning effectively and efficiently, the organization of learning contents is the next important factor; and the learning management system (LMS) is appropriate for this purpose.

LMS enables us to present all of the learning contents at once, organize them in a variety of settings, to deliver them in various forms. About the content organization, learning contents can be presented both as a whole and as separated learning units simultaneously. Seeing learning contents that way, learners have inputs to plan their learning path. About learning contents being delivered in various forms, learners can apply various cognitive activities into learning contents and be supported in absorbing knowledge via multiple senses.

Reflection is to look back into learning history to gain experience. LMS records a history of learning interactions between learners and the materials, which are insightful sources for reflection.

B. Mastery Learning

The awareness course designed in this paper strives to provide learners not only with cybersecurity knowledge but also a training environment in which the learners can form themselves abilities to counter cybersecurity issues in daily internet usage. To achieve that purpose, we choose a mastery learning approach to implement the course. Mastery learning theory says that learners, when learning a subject, can master that subject on the following four conditions:

- The learners are given a sufficient amount of time to learn;
- Instructions are systematically organized;
- The learners can absorb the instructions and persevere to continue learning from corrective feedback;
- The criteria of mastery are clearly defined [7].

Learners differ in their usage of time, and they also perform different cognitive activities on learning resources to reach the mastery level. LMS supports this diversity of learning approach by giving out training goals, preparing learning resources that learners are free to use in their own time setting, and providing feedback to virtually accompany learners throughout their learning path.

C. Gamification

Gamification is the application of game elements or game mechanisms into real-world contexts. In education and training contexts, empirical studies show that gamification helps learners absorb and retain knowledge longer and deeper [8]. Gamification provides learners with three benefits: motivating learners, relaxing their minds, and strengthening their habits.

Fig. 1 illustrates how SRL, game elements, and learning contents interoperate to bring about the benefits mentioned above. When learners self-regulate their learning, motivation plays a significant role in stimulating their autonomy and progress for learning, and game elements are the stimuli. Motivation for a learner is both intrinsic and extrinsic. Intrinsic motivations can be a growth of knowledge, a gained ability in a specific field of expertise, an enlightened and enlarged intellect. Extrinsic motivations can be the recognition from peers about high performance, rewards for

overcoming challenging exercises, points earned for every step of progress. It is ideal that self-regulated learners motivate themselves intrinsically when learning.

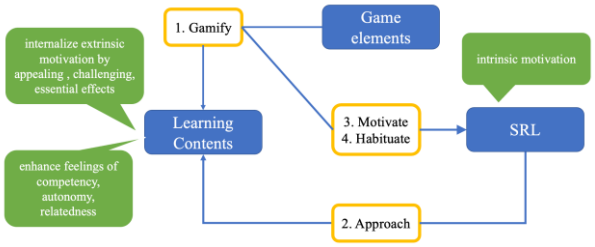

Fig. 1. Interoperations between gamification, course contents, and SRL.

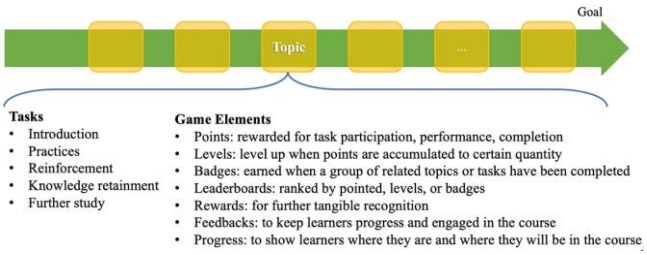

Fig. 2. Game elements used in a course.

III. Course Design

The course aims to raise learners' awareness of cybersecurity domain, enhance the learners' ability to recognize cybersecurity issues and provide practices to prevent cybersecurity attacks. The course is also designed in a manner by which learners can learn effectively by themselves.

A. *Interoperation between Gamification, Course Contents, and SRL*

In order that students can learn at their own pace under their regulation, the course is designed based on SRL principles [4]. Then, the application of SRL principles is empowered via gamification on learning management systems such as Moodle.

The course comprises lessons gamified with elements that encourage and support learners to self-regulate their learning process. As the SRL approach has three key activities: planning, monitoring and controlling, and reflection, the application of gamification into the course should be designed to motivate the learners to perform these SRL activities. How do we design such a course?

The course runs by the interoperation between game elements, learning contents, and SRL as presented in Fig. 1. The learning contents comprise lessons gamified by game elements that provide learners with extrinsic motivation and then gradually invoke the learners' intrinsic motivation to encourage their SRL.

B. *Course Structure*

The contents are separated into small units of learning. Each unit contains learning tasks of a specific topic to arouse awareness, exercises to reinforce learners' understanding of the lessons, retain knowledge, and further readings to encourage further study. A first brief view through the course might focus learners' attention on cybersecurity issues and inspire them to study specific topics deeply in a self-regulated learning manner. When being interested, learners transform their awareness of cybersecurity subject matters to build up recognizing and preventing cybersecurity issues. Each learning unit comprises five main parts: Introduction, Education, Reinforcement, Checklist for knowledge retainment, and Further study.

The *Introduction* attracts learners to a topic by telling the learners about what area of cybersecurity the topic is, which goal they are expected to achieve, the rationale for learning.

The *Education* contains materials and resources of different types to facilitate learners to obtain the topic's knowledge. The learning materials and resources are, but not limited to, video clips, textbooks, reference books, quizzes, and games, which bring knowledge to learners via different senses.

The *Reinforcement* offers use cases for learners to practice what they have learned and familiarize their mindset and skills with that knowledge

About the *Checklist*, when having taken the education and reinforcement activities, learners use a checklist to distill knowledge

About the *Further Study*, after learning a topic, learners might have the interest to know further, and this section supports the learner to do that.

C. *Game Elements*

To encourage learners, game elements offer learners visible signs of their efforts, which motivate them to progress their learning. Appropriate application of such game elements helps learners see what they have learned with real intrinsic growth of their knowledge and intellect, and they gradually develop their own intrinsic motivation. Learners are motivated when they know where they and will be, which ability they have gained, feedback for their development, achievements of scores and performance, and community in which they belong. For these reasons, and also widely agreed and applied in educational settings [9], the following game elements will be used: Points, Badges, Leaderboards, Rewards, Feedback, and Progress. How the game elements contribute to the course is presented in Fig. 2.

D. *Course Design Framework*

The course structure and game elements are interwoven as presented in the following course design framework (see Fig. 3). The framework illustrates the roles of game elements and their use in relation to corresponding learning tasks to help learners self-regulate their learning in each learning task within a topic, in a topic of the course, and throughout the course.

As learners traverse through the course, points are awarded to them for their interactions with the course. The interactions vary from visiting learning materials, joining forum discussions to doing quizzes, reviewing knowledge, and the like. The points are the intangible signs of extrinsic motivation, which shows learners' accumulation of their engagement and learning activities.

Next are badges. Badges are the recognition of the accomplishment of related tasks or topics. By earning badges, learners are motivated because of the recognition that they are capable of performing skills, and such recognition shows

their intrinsic growth of knowledge.

When the points and badges are accumulated up to a certain amount, learners see their levels regarding their peers in the leaderboard. The leaderboard creates a competitive environment [8] to stress a certain amount of pressure on learners, motivating learners to reach superiority, and acts as a reminder to keep learners' minds in the game.

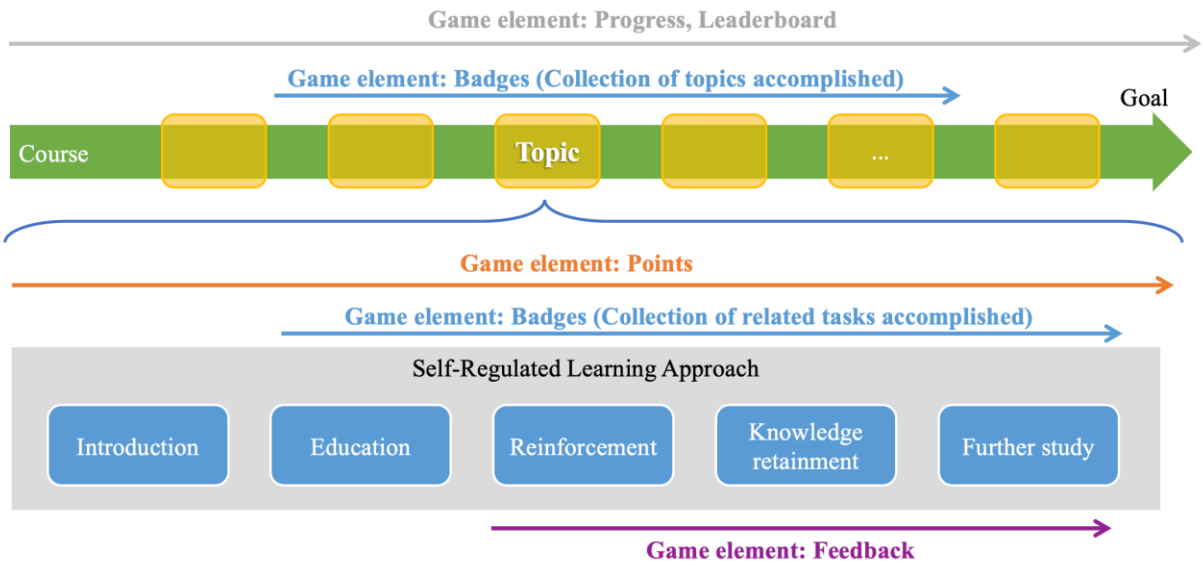

Fig. 3. Course design framework.

Self-regulated learning might be challenging, and learners might lose their way when encountering difficulties. Hence, feedback is given constantly to learners in order that the learners have a sense of receiving necessary support and always benefit from their self-regulated learning. The game element of feedback is used in *Reinforcement*, *Knowledge Retainment*, and *Further Study* learning tasks where learners apply knowledge into practice and quizzes.

Commitment to the course requires learners' time and effort, and the learners might be tired, get bored from the course, or lose track of where they have been and where they will go next in the course. To provide the learners with a course map, the game element of progress plays such a role.

Finally, all points and badges collected will not have any moving-to-action meanings if they are just intangible signs of motivation. To actually motivate learners, the accumulated points and badges should be able to redeem as tangible recognitions, for example, specific accumulated points redeeming an account for cybersecurity textbooks, certain collect badges meaning that a learner is invited to deliver a workshop about a particular security topic.

E. Course Topics

The training course designed in this paper targets graduate students in a research institution.

Internet services that the target learners mostly use are mail, social networks, e-commerce, search engines, and so forth. Most of the students are familiar with internet services, yet they might neither be aware of internet security threats nor classify sources of those threats and how to prevent them effectively.

The goal of the course is to inspire students to study further about information security after a brief tour through the course. The course objectives are that after a quick tour through the course, learners are aware of the necessity of information security of knowledge in keeping themselves from harmful misuse, and they are inspired to study information security further in a self-regulated manner. The topics shown in Table I will be addressed.

TABLE I: COURSE TOPICS AND OBJECTIVES

Topic	Objectives
Passwords	Awareness of weak passwords easy to be guessed
	Awareness of massive loss of information when using the same password for different internet accounts
	Awareness of what a strong password is and the necessity to use strong passwords
	Awareness of using password management tools when having many passwords
	Practice/Skill to set strong passwords
Unauthorized access	Awareness of harmful effects when accessing other persons' account without the other's consents
	Recognition of signs of unauthorized access
	Practice/Skills to prevent unauthorized access

Topic	Objectives
The importance of up-to-date OS	Awareness of security vulnerability of OS when it is outdated. Awareness of how updating OS prevents cybersecurity risks Practice to keep OS up-to-date
Usage of Antivirus software	Awareness of computers without antivirus software, more likely to be infected by viruses Awareness of harmful effects when computers are infected by viruses Awareness of how antivirus software protects the computer from viruses Practices/skills to reduce computers from exposure to virus infection risks
Phishing email	Awareness of how likely it is to have fraud or phishing emails Awareness of harms caused by opening phishing emails Recognition of phishing emails Practices/Skills to handle phishing emails
Correct management of Personal Information and research data	Awareness of signs about leaking personal information Awareness of potential harms from leaking personal information Practice/skills to refrain from leaking personal information
Illegal use and disclosure of others' work	Awareness of harmful effects when illegally copying author's work and distributing them online Recognition of signs of illegal behaviors related to copy and distribution of author's work Practices/Skills to refrain from making copies of author's work and distributing them
Cautions about Social Network Services	Awareness of widespread and permanency of information when it is posted online Awareness of harmful effects from inappropriate information being posted on social network services Practices/Skills to prevent the dissemination of inappropriate information on social networks
Prevent access from outsiders	Awareness of potential information security risks when outsiders can access an organization's network Recognition of behaviors that are likely to open doors for outsiders to access internal network Practices/Skills to prevent authorized access from outsiders
Caution about law violating and security-threatening applications	Awareness of harmful effects that security-threatening applications might cause to users and network Recognition of security-threatening applications with their harmful behaviors Practices/skills to refrain yourselves from using such applications

IV. Course Implementation

Currently, our institution, JAIST, has provided students with cybersecurity contents in three approaches: (1) using a short video to instruct cyberspace etiquette in academic contexts, (2) using bulleting boards on campus to remind cyberspace etiquette, and (3) delivering self-study courses on JAIST LMS. These approaches mentioned above play an important role in drawing attention to cybersecurity matters. The proposed course of this project adapts to the content of the above video and aims to enhance learners' awareness and provide them with practices to develop habits and skills in cybersecurity.

We will implement the course into and deliver the course via JAIST LMS Moodle [10] since the students are familiar with Moodle and there are appropriate plugins—additional applications able to be installed into Moodle for adding extra functionalities to Moodle—that support gamification to support self-regulated learning as mentioned in section III.C.

The following are screenshots of the sample course on Moodle. Let us walk through the streamline of the course. The course begins with a presentation of all topics, which demonstrates the idea of showing the learning journey and checklist of learning objectives. The purpose of this presentation is that each of these content is checked out after learners have finished all of their tasks (as presented in Fig. 4).

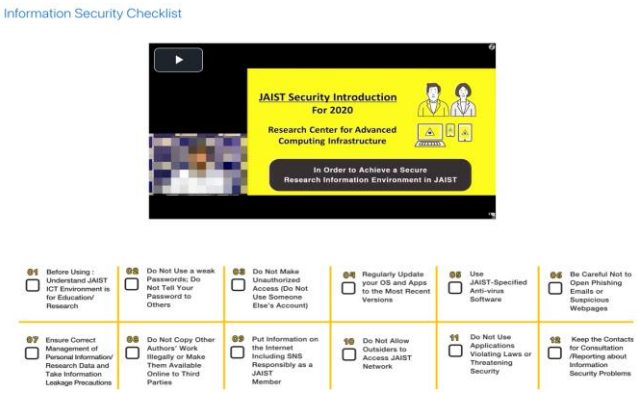

Fig. 4. Presentation of learning journey and learning objectives checklist.

Learning the course, students will join tasks varying from watching video clips, trying online tools, doing quizzes, reviewing with a checklist. These types of content (demonstrated in Fig. 5) will be further visually designed and presented to attract learners' attention.

During the learning process, students' interaction with the course, such as watching video clips, reading materials, doing quizzes, are accumulated as progress and then represented via available plugins such as the Level up! [11], Badges [12] (displays shown in Fig. 6). Seeing progress motivates students to persevere with their learning.

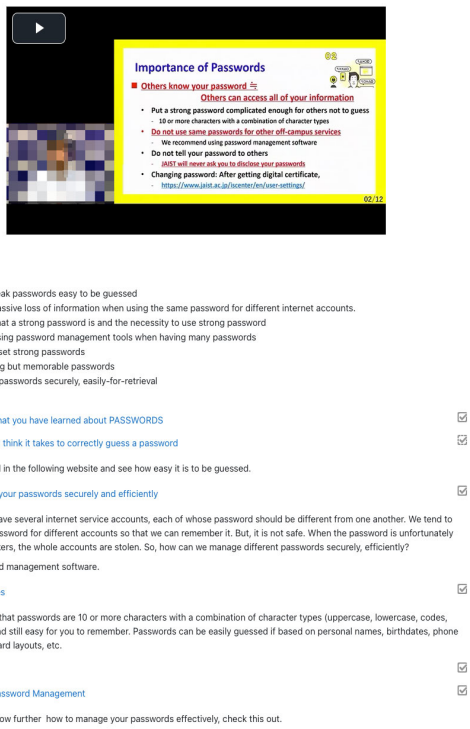

Fig. 5. Learning task types.

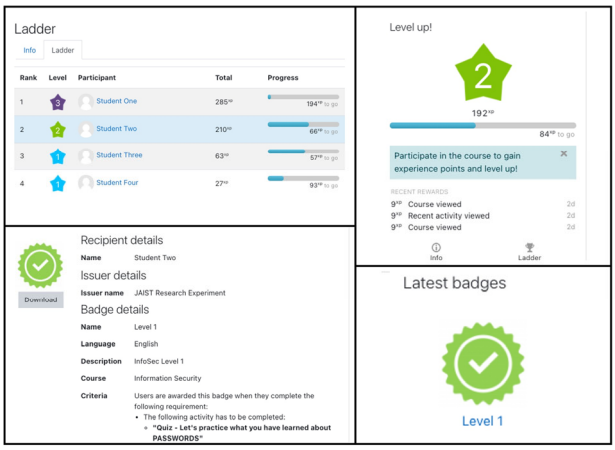

Fig. 6. Plugin Level Up showing learning progress as a leaderboard, and Plugin Badge showing learning achievements.

With such the content organization, the course is expected to assist students in the following process:

- Step 1: Motivate students to attract their attention to content. Students are motivated when realizing the necessity of learning topics, the facilities that are available for them to self-study, and the study community to which they belong are related;
- Step 2: Encourage the students to plan the learning process. Checklists, milestones, and indicators of competency are means to encourage the students to plan their learning;
- Step 3: Support them in learning management and knowledge retainment. The support is delivered by quizzes, practices, challenges, and rewards of different types to prevent boredom and monotony;
- Step 4: Encourage them to review their gained knowledge and their learning approach. Checklists, self-reports, surveys can be used as a reminder to help the students reflect on what they have learned and distill knowledge into their possession.

V. Conclusion

We have walked through the three underlying principles of self-regulated learning, gamification, and mastery learning, as well as detailed steps applied to structuring an online course to help them self-study effectively. Although cybersecurity is a challenging and difficult-to-digest domain for learners to self-study, we believe that our proposed framework promises to design effective gamification-based cybersecurity awareness courses for self-regulated learners to obtain basic concepts of cybersecurity. Future work from this paper is that we implement on Moodle an online course that delivers the aforementioned ten topics of cybersecurity to students at our institute, JAIST.

Grounded on self-regulated learning and gamification and mastery learning principles, the proposed framework aims at two purposes: building motivating and effective online courses, and from learning the courses, learner's SRL skills being strengthened. To evaluate the framework according to these purposes, we assess the to-be-implemented online course on Moodle from three perspectives: learning content, SRL ability growth, and game elements' effectiveness.

Firstly, the learning content. The proposed topics are selected according to JAIST's analysis and consideration of common threats and vulnerabilities that JAIST students and staff encounter daily. But the learning content is not static; it should be both stable regarding effectiveness and adaptive to learners' cybersecurity needs. Therefore, we assess the appropriateness of the learning contents by surveying learners' opinions about course contents and conveying quizzes to check learners' competency on cybersecurity awareness levels. We also open feedback channels to encourage learners to give suggestions and concerns, which are valuable sources of information for modifying the learning content.

Secondly, the effectiveness of a course is reflected on the learners' obtainment of knowledge, and because learners self-regulate their learning on the course, it is followed the learners' acquisition of knowledge results from the learners' SRL ability. LMS records online learning behaviors and their effects, from such activities as reading learning materials, watching video clips, doing quizzes, posting messages on a forum resulting in cognitive scores. Analyzing such sequences of learning behaviors and their corresponding results brings out a manifestation of SRL patterns on the scale of each learning unit and of a whole course. The relations between the learners' SRL patterns and the learners' performance on a course demonstrate their SRL ability.

And thirdly, as discussed in the above sections, the game elements play the role of providing learners with extrinsic motivation in order that the learners gradually grow intrinsic motivation to engage in the course and to progress their learning. Therefore, assessing their contributions to learners' performance is needed so that we know how qualitatively and quantitatively the game elements are appropriate to enhance learners' motivation and to help them absorb knowledge effectively rather than discouraging the learners. Since the effectiveness of game elements is reflected on learners' growth of extrinsic and intrinsic motivation, assessment of such effects can be conducted directly by self-reports from the learners and indirectly by the level of engagement of the

learners in the course and their end results from the course.

Not constrained within the cybersecurity domain, the framework can potentially be applied to developing gamification-based courses for self-regulated learners in other study fields to help learners study with extrinsic and intrinsic motivation for the growth of knowledge and maturity of the mind.

Conflict of Interest

The authors declare no conflict of interest in conducting this research.

Author Contributions

Tuan M. Tran conducted the literature review, developed the course design framework, and wrote the manuscript drafting. Razvan Beuran revised the manuscript with great critical correction and gave final approval on the final version. Shinobu Hasegawa counseled the course contents to be developed. All authors have read and approved the final manuscript.

Funding

This work was supported by JSPS KAKENHI Grant Number 18H03346.

Acknowledgment

The authors would like to express their thanks to the Japan Advanced Institute of Science and Technology for supporting this research.

References

[1] J. Marron, V. Pillitteri, J. Boyens, S. Quinn, G. Witte, and L. Feldman, "Approaches for federal agencies to use the cybersecurity framework," NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2020.

[2] Z. Tan, R. Beuran, S. Hasegawa, W. Jiang, M. Zhao, and Y. Tan, "Adaptive security awareness training using linked open data datasets," *Education and Information Technologies*, 2020, doi: 10.1007/s10639-020-10155-x.

[3] M. Wilson, J. Hash, and Technology NIST, "Nist 800-50," *Nist*, no. October, p. 70, 2003.

[4] M. Tran and S. Hasegawa, *Self-Regulated Learning Recognition and Improvement Framework*, 2021, doi: 10.22492/issn.2186-5892.2021.40.

[5] J. H. Flavell, "Metacognition and cognitive monitoring: A new area of cognitive–developmental inquiry," *American Psychologist*, vol. 34, no. 10, pp. 906–911, 1979, doi: 10.1037/0003-066X.34.10.906.

[6] E. Panadero, "A review of self-regulated learning: Six models and four directions for research," *Frontiers in Psychology*, vol. 8, no. APR, pp. 1–28, 2017, doi: 10.3389/fpsyg.2017.00422.

[7] B. S. Bloom, "Mastery learning," in *Mastery Learning: Theory and Practice*, J. H. Block, P. W. Airasian, B. S. Bloom, and J. B. Carroll, Eds. New York: Holt, Rinehart and Winston, 1971, pp. 47–63.

[8] L.-M. Putz, F. Hofbauer, and H. Treiblmaier, "Can gamification help to improve education? Findings from a longitudinal study," *Computers in Human Behavior*, vol. 110, p. 106392, 2020, doi: 10.1016/j.chb.2020.106392.

[9] F. F.-H. Nah, Q. Zeng, V. R. Telaprolu, A. P. Ayyappa, and B. Eschenbrenner, "Gamification of education: A review of literature — HCI in business," Springer, vol. 8527, pp. 401–409, 2014, doi: 10.1007/978-3-319-07293-7.

[10] Moodle. (2021). *Solutions for Higher Education*. [Online]. Available: https://moodle.com/solutions/higher-education/

[11] F. Massart. (2021). Level up! — Gamification. *Moodle*. [Online]. Available: https://moodle.org/plugins/block_xp

[12] Moodle. (2021). *Badges*. [Online]. Available: https://docs.moodle.org/311/en/Badges

Copyright © 2023 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).