Chapter 11
Design and Develop a Cybersecurity Education Framework Using Capture the Flag (CTF)

Li Jing Khoo
Sultan Idris Education University, Malaysia

ABSTRACT

The rise of cyber threats is projecting the growth of cybersecurity education. Malaysian students who are interested in studying computing and information technologies suffer from knowledge and skill gaps because the earliest exposure of formal computer knowledge happens only at tertiary level education. In addition, the ever-evolving cyber landscape complicated the gaps and exposure. This chapter reveals the learner's motivation factor through an exploratory study in a national level cybersecurity competition. By simulating a real-world cyber landscape, a customized cybersecurity game, Capture the Flag was designed, developed, and validated as an experiment to study the relationship between learners' motivation and achievement level.

INTRODUCTION

Cybersecurity education is blooming to produce the next generation of experts in tackling global cyber threats (Ford, Siraj, Haynes, & Brown, 2017). Students are the focus of teaching and learning (T&L) process but they are suffering the skill gap in catching up with fast evolving cybersecurity landscape (Endicott-Popovsky & Popovsky, 2014). Advanced countries such as the United States, structures a holistic framework called the National Initiative for Cybersecurity Education (NICE), under the National Institute of Standards and Technology or NIST (Newhouse, Keith, Scribner, & Witte, 2017). This framework would foster a partnership between government, academia, and the private sector, as it focuses on cybersecurity education, training, and workforce development (Newhouse et al., 2017).

DOI: 10.4018/978-1-7998-7705-9.ch011

In Malaysia, the Ministry of Science, Technology and Innovation has developed a National Cyber Security Policy (NCSP) in 2010 (Razana & Shafiuddin, 2016). However, when the NCSP and the NICE are compared, there is a gap of actions needed from different units in the policy of Malaysia to achieve an internationally expected security level, especially a missing framework for cybersecurity education. Without the support of a cybersecurity education framework and the vast topics covered in cybersecurity, students who pursue formal academic qualifications in Malaysia may receive inconsistent knowledge and skills as compared to those in advanced countries. In practice, students in Malaysia solely depend on syllabus implemented by individual educational institutions they join. In countries that implement the K-12 education system, such as USA, cybersecurity concepts are commonly introduced at elementary level (see National Initiative for Cybersecurity Education, 2017). In contrast, students in Malaysia do not take formal lessons in schools; instead, they begin learning ICT skills and specialized cybersecurity topics after taking courses at tertiary level.

This chapter offers a potential feature to fill in the gap in the NCSP. This feature can support the cybersecurity education strategy through Capture the Flag (CTF) competitions as a dynamic T&L approach. Cybersecurity conferences frequently hold CTF competitions but the effectiveness of CTFs as a T&L approach were subjective in the eyes of academic researchers (Chapman, Burket & Brumley, 2014; Tobey, Pusey, & Burley, 2014). CTF is a competition where participants must obtain the highest points (flags) from a target or a server within a predetermined time limit (Chothia & Novakovic, 2015). It simulates the environment of a hacking incident where participants play either the role of a hacker or a forensics investigator, depending on the nature of given challenges. Organizers of CTF may customize the gameplay with unique scoring systems, duration of competition, rewards etc. Data generated from a CTF competition can be studied to determine the effectiveness of content delivery, assessment analysis and progress monitoring (Ford et al., 2017; Silva et al., 2014). The competition simulates a sports game where a player gains experience of hands-on tools against real machines, instead of controlling an avatar in the game world (Chapman et al., 2014; Ford et al., 2017). To win a CTF competition, a player needs to strategize and contribute to his or her team in the process of achieving the goal (Chapman et al., 2014).

To certain extent, CTF emulates the process of a physical sports game in the Olympics, such as racket sports, ball games and sprinting (Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). Like professional athletes who train rigorously, CTF players spend intensive hours in solving simulated cybersecurity challenges, gearing towards their best performance in actual competitions. When CTF competitions are organized for educational purposes, CTF should consist structural elements of educational games, including intended learning outcomes, designated game space, appropriate challenge types, engaging interactions, and efficient assessments (Tan, 2015). With reference to criteria of good educational games, criteria of organizing a national level CTF competition were gamified by following a five-step gamification approach (see Tan, 2015), in order to match learning content to an assessment matrix. The assessment matrix is based on a performance criteria that calculate total of flags being submitted in the session. Participants' motivation factors (feel challenged and satisfaction in solving challenges) and CTF assessment criteria (high score and rewards) enable CTF to present an opportunity for experimental teaching practices and field studies. In this sense, the nature of CTF activities are measurable and results of data analysis are generalizable. Observations can study the participants' reaction during competitions (Fink, Best, Popovsky & Endicott-Popovsky, 2013). With the production of assessment plan and teaching guide after the mappings, several assessment sessions will be built from the CTF game to support the research. The indispensable result from this research will contribute to the effort of enabling Malaysia