A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia

Arash Ghazvini
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia,
43600 UKM, Bangi, Selangor, Malaysia

Zarina Shukur
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia,
43600 UKM, Bangi, Selangor, Malaysia

***Abstract*—This paper aims to develop an information security awareness training program for the healthcare industry to ensure the appropriate protection of electronic health systems. Serious games are primarily designed for training purposes rather than pure entertainment. Serious games are proven as an effective training approach for awareness programs. Serious games benefit learning as the games are fun to play and motivate learners to participate and interact with learning activities. Developing a serious game requires the revision of adequate guidelines that identify all characteristics to be incorporated in such games. Thus, this paper reviews serious game models that have been constructed as game development guidelines. To this end, a serious game is developed and implemented at a selected healthcare organization.**

Keywords—Serious game; information security; awareness training program

I. Introduction

As a new approach in developing information security awareness training programs, computer game-based training is proven as an effective and engaging program [13][11][7][15]. Computer games provide engaging interfaces that enhance training, draw more trainees in, and simulate a variety of scenarios [16][12]. They provide a simulation environment with pre-defined scenarios that motivate players to try different approaches to run the system [1]. The objective for game players is to improve their ability in decision making and learn how to cope with challenging situations. Unlike traditional training programs that focus on the technical aspect of a system, this new approach improves the decision-making skill of game players for handling challenging situations [4]. Computer games give employees an experience by offering them a platform to apply their decisions before those decisions are actually implemented in the real place. For instance, computer games teach users about healthcare values, the information they have access to, the information they are allowed to share, as well as behaviors they are supposed to demonstrate to protect electronic health records [4]. Computer games are effective in the way that they create a platform for players to practice their behaviors and handle the consequences of their decisions in a virtual environment.

II. Serious Games

Serious games (or applied games) are games primarily designed for training purposes rather than pure entertainment. When it comes to training purposes, computer games should be able to integrate educational elements, content, and multimedia while being playable to users with a pleasant interface [14]. References [5][10][19][3] emphasized the educational advantage of a serious game. "The serious games application is intended to help professionals, as well as enabling users to enjoy themselves through straightforward, real interaction while learning how to cope in several real social situations".

III. Serious Game Models

This paper develops a serious game called InfoSecure as a training delivery method for Hospital Universiti Kebangsaan Malaysia (HUKM). The aims are to raise HUKM employees' awareness of information security and help them adhere to appropriate behaviors that do not compromise the security of information assets. However, the development process requires adequate guidelines that include all characteristics that should be incorporated in a serious game. Therefore, it is necessary to review available serious game models. The following part briefly discusses serious game models.

Reference [6] introduced a model that explains the relationship between learner and serious games. The model is too basic and designed for fundamental games. It does not provide a detailed design for optimal learning. Reference [8] proposed a framework that supports teachers' evaluation of serious games. The framework only discusses game evaluation but not game design [17]. Reference [9] developed a framework based on classroom teaching. This model imitates the textbook style and does not offer rooms for exploratory learning. Reference [2] introduced a model to identify interface requirements of a serious game. However, the model is too general with a little guideline for designing a serious game. Reference [17] offered a model that is highly dependent on a software called Emergo. His model remains at the theoretical stage and does not provide any design solution to use other game design tools.

Reference [18] proposed a serious game model that is the most efficient and effective model for serious games. Yusoff's

model is based on the review of learning and pedagogy perspectives in combination with the games. This conceptual model is developed to be used by game designers for efficient game development as well as the educational practitioner when designing serious games for effective learning. The conceptual framework proposed by Yusoff is the basis for InfoSecure serious games design (Figure 1). The gray boxes are entities added to the original model to explain how the model is used to develop a serious game for information security awareness training programs.

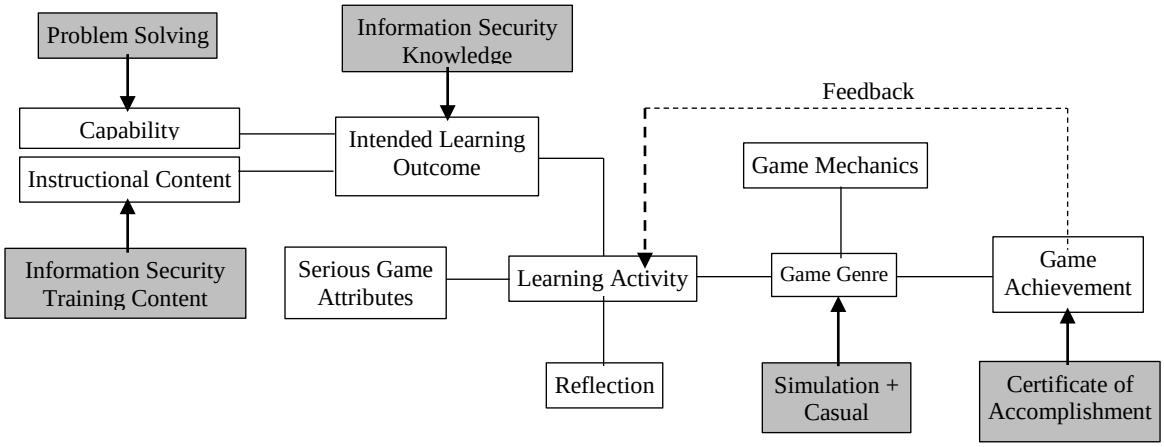

Fig. 1. Serious Game Model Adapted from Yusoff (2010)

A. Capability

Capability refers to the cognitive skills to be developed by employees from playing a game. In training, conative problem-solving skills attempt to decrease inappropriate behaviors by developing a new perspective and enhancing knowledge about the subject matter. In the context of information security, the aim is to help employees adhere to appropriate behaviors that do not compromise the security of information assets.

B. Instructional Content

Instructional content refers to the subject matters that must be learned by the employees. The InfoSecure game teaches employees how to protect healthcare information assets. The reason why InfoSecure is developed is due to the failure of the employees to understand and maintain the security of information assets.

C. Learning Activities

The learning activity is the activity designed to keep the learner engaged and learn in the game world. InfoSecure games provide different activities to keep employees engaged and attracted. For example, the story of the InfoSecure topic is to feed a fish by answering all questions correctly and to avoid catching the bait. The most important fact is to ensure employees stay engaged without getting bored, and show interest to play the game for learning.

D. Intended Learning Outcomes

Intended learning outcome refers to the objective achieved by the employees from playing the serious game. By the end of the game, employees will be able to use and apply the newly acquired knowledge in their daily work activities. The objective is to enhance the employees' knowledge about risks and hazards associated with information security.

E. Reflection

Reflection is where the learner thinks about the purpose of the learning activities that have been undertaken. For healthcare employees, understanding the importance of information security is a motivational factor to participate in awareness training programs.

F. Game Genre

Serious games can be of any genre with the ultimate objective of education. Each genre has its own characteristic that makes it attractive. A combination of simulation and casual genres is used to design InfoSecure. Simulation games are favored as they simulate the real work environment, which allows users to make mistakes and learn from those mistakes without worrying about the consequences of their actions as they would in real life. However, serious games also require the flexibility and fun aspects that usually appear in casual games.

G. Game Mechanism

Game mechanics are the game operations, and the purpose of this notion is to enable the game to be more fun, enjoyable, and more engaging for the player. There should be at least one game mechanism for each genre. The simulation genre focuses on a single activity and attempts to replicate the real world experience. The outcomes can be highly consistent with a real-life experience or exaggerated. Simulation games place players as decision-makers to manage the simulated situations. Moreover, games with the casual genre are easy to play and master. The design of these games is adopted from conventional games such as chess and cards games. The interface of the game should be very simple. The common goal in casual games is to score.

H. Serious Game Attributes

It refers to the attributes of a serious game that support learning and engagement. Yusoff (2010) identified twelve important attributes of a serious game. Table I explains how

these attributes are incorporated into the design of the InfoSecure game.

TABLE I. SERIOUS GAME ATTRIBUTES

Attribute	Description	The InfoSecure Game
Incremental learning	The learning material is delivered in an incremental way	The target audience is general employees with basic knowledge of information security. Therefore, the training content is developed respectively.
Linearity	Learning is arranged sequentially	InfoSecure consists of eight topics; each covering one topic of the policy.
Attention span	Duration for learning concentration	InfoSecure breaks up learning sessions into several intervals to produce effective learning. The time spent on each topic is about 5 minutes.
Scaffolding	Support and help during the learning process	Not applicable.
Transfer of learned skills	Applying skills to new learning based on previous learning	Each topic is designed to have one level to cover one distinct topic.
Interaction	Engagement in learning	InfoSecure is a combination of simulation and casual genre.
Learner control	Self-learning and active learning based on the learner's pace	There are eight topics. The player has the freedom to select and play any of the topics.
Practice and drill	Learning activities and exercises within the game	A topic can be played repeatedly until the full score is achieved.
Intermittent feedback	Inform learners of their progress in learning	Players' correct or wrong answers to information security questions are indicated by √ and × marks.
Reward	Incentives for the learner	A certificate of accomplishment is rewarded when full scores are achieved.
Situated and authentic learning	Placing the learner in an authentic learning environment	The themes and backgrounds of InfoSecure games are relevant to the healthcare work environment.
Accommodating the learners' style	Learning to suit learners' preferences	Serious games are suitable to be played by all types of learners.

I. *Game Achievement*

Game achievement is the level of the learners' achievement in playing these games. It can be indicated by the game scores, and it gives the pleasure of rewards. The game achievement or score indicates the level of learners' knowledge of the game. In the InfoSecure game, a certificate of accomplishment is rewarded when full scores are achieved for all the topics.

IV. INFOSECURE CONCEPTUAL MODEL

Figure 2 is the conceptual model of the InfoSecure serious game developed in this paper. Because this is a conceptual model, it can be used as a framework that visually represents the arrangement of the InfoSecure game elements. The conceptual model consists of nine parts: 1) Capability, 2) Instructional Content, 3) Learning Activity, 4) Reflection, 5) Serious Game Attributes, 6) Game Genre, 7) Game Mechanism, 8) Evaluation, 9) Game Achievement.

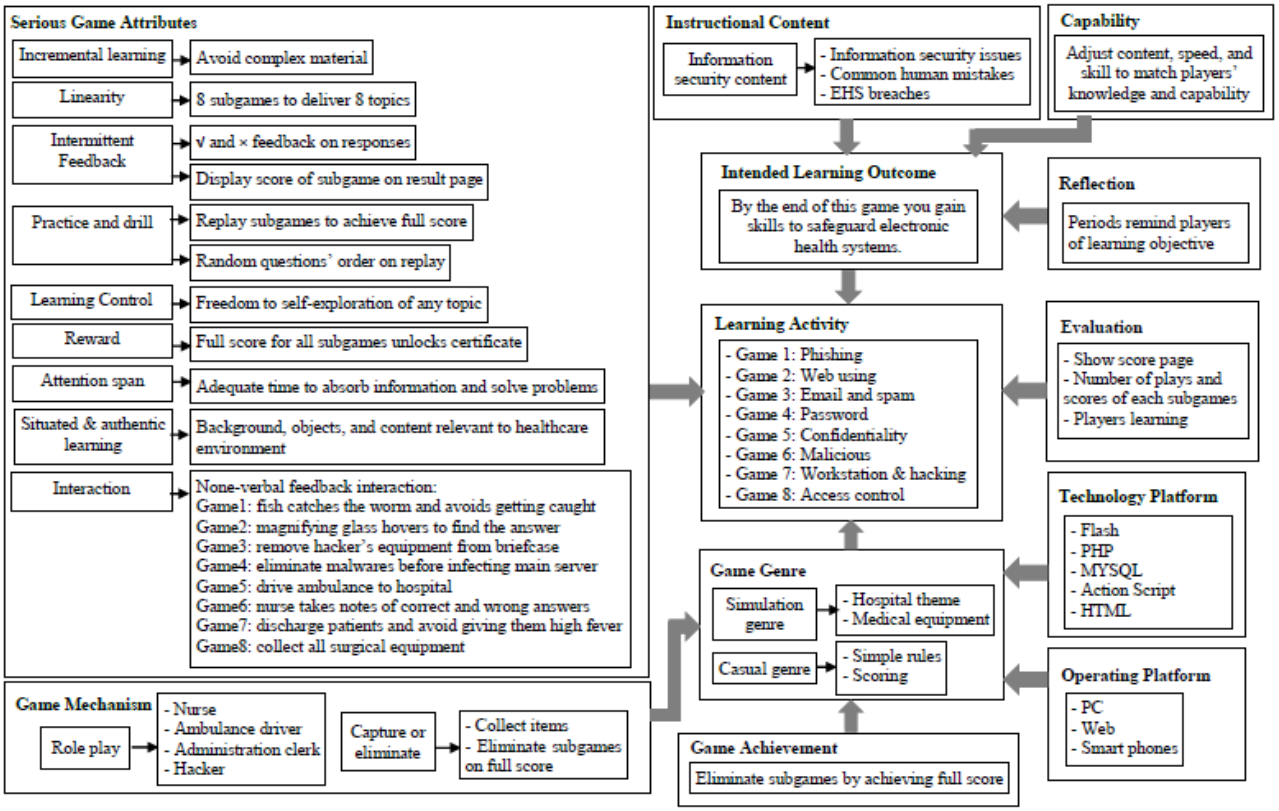

Fig. 2. InfoSecure conceptual model

Table II presents the implementation of the serious game model elements in the InfoSecure game. It explains how these elements are used to develop the InfoSecure game in this study.

TABLE II. IMPLEMENTATION OF THE SERIOUS GAME MODEL ELEMENTS IN THE INFOSECURE GAME

Serious Games Model Elements	**Implementation in InfoSecure Game**
A. Intended Learning Outcomes	The intended learning outcome of playing the InfoSecure game is displayed on the homepage. The intended learning outcome is defined as follow: *By the end of this game, learners will be able to protect/ promote healthcare's information asset/security.*
B. Capability	InfoSecure is auto-adjusted to match player's knowledge and capability. Since this particular game is not an action-based genre but closed to a direct simulation genre and the target user capability is already known in advanced therefore it is not regulated to be a self-adjusted system to correct the content delivery in order to match to the learner capability.
C. Instructional Content	The InfoSecure game aims to teach learners about information security concepts. The instructional content that is intended for players to learn covers: 1) learning about information security issues 2) learning about human roles to maintain the security of information 3) learning how to prevent information breaches.
D. Learning Activities	The InfoSecure game consists of eight topics, each covering one information security issue in the healthcare. It provides different activity in each topic to keep employees engaged and attracted. For example, the story of game number 1 is to feed a fish by answering all questions correctly and avoid catching the bait. The important fact is to ensure employees stay engaged without getting bored and to ensure that they show interest in playing the game for learning.
E. Serious Game Attribute	
• Incremental Learning	The targeted audience is general employees with basic knowledge of information security. Therefore, training content is developed simple and easy to understand. InfoSecure breaks up learning sessions into several intervals to produce effective learning.
• Linearity	InfoSecure consists of eight topics, each covering one information security issue of the firm.
• Attention Span	The timing given to absorb information and solving the problems must be adequate enough. If the timing is too short, extend the timing. If the learning process too complicated, modify it to make it simple. The training time fluctuates depending on the number of questions set by the instructor. However, there is no time limit for players to finish the game. Adequate time to absorb information and solve problems. The player can leave and come back at any time to resume with training. It helps players digest new information and answer the questions.
• Transfer of Learnt Skills	Not applicable to InfoSecure. Each topic has a different scenario and covers different information security topics. Players do not need to acquire new skills to apply at the next level.
• Interaction	InfoSecure provides players with feedback interaction. Game1: fish catches the worm and avoids getting caught on the hooks Game2: magnifying glass determines if the selected answer is correct or wrong Game3: remove hacker's equipment from the briefcase Game4: eliminate malware before infecting the main server Game5: drive the ambulance to the hospital Game6: nurse checks if selected answer is correct or wrong Game7: discharge patients and avoid giving them high fever Game8: collect all surgical equipment
• Learner Control	There are eight topics on eight information security topics. Player has the freedom to select and play any of topics. InfoSecure provides self-learning to suit players' pace and experience.
• Practice and Drill	A topic must be replayed until the full score is achieved to eliminate the topic. Every time player replays a topic, questions are automatically reordered to avoid memorizing the pattern of correct answers.
• Intermittent Feedback	Fixed ratio feedback suits the strategy of InfoSecure. A feedback would be given after each response from a learner and at the end of each topic. Correct answers will be indicated by √ and wrong answers by × marks. After the player responded to all questions, the result page appears to show the topic of topic, username, and score. Once the full score is achieved for a topic, the topic will be eliminated from the homepage indicated by the √ mark.
• Reward	A certificate of accomplishment is rewarded when the full score is achieved for all topics.
• Situated and Authentic Learning	Incorporate familiar background, objects and common examples in games content, to relate it to the healthcare environment.
E. Game Genre	InfoSecure is developed based on characteristics of simulation and casual genres. Games with simulation genre are favored as they simulate real work environment which allows users to make mistakes and learn from those mistakes without worrying about the consequences of their actions as they would in the real life (Apperley, 2006). The serious game also requires the flexibility and fun appeared in casual games in order to release users' boredom

	and tiredness [13]. The design of these games is adopted from conventional games such as chess and cards games. The interface of the game should be very simple [13]. The common goal in casual games is to score. To fulfill the requirement of simulation genre, hospital theme is used as the main theme of InfoSecure, and medical objects are used in the game design. To fulfill the requirement of the casual genre, each topic is differently designed to avoid boredom and to make the game challenging and fun. Nevertheless, all topics hold the same goal of raising employees' awareness towards information security. InfoSecure is designed simple with familiar background and graphics and is easy to play and master.
F. Game Mechanism	Role-playing: learners get to play as a nurse, ambulance driver, administrative clerk, and computer hacker. Capture or eliminate: in order to achieve the certificate of accomplishment, the player must eliminate all eight topics by answering all questions correctly.
G. Technology Platform	The InfoSecure game is developed with Adobe Flash. Aside from being interactive, the flash timeline allows developers to create most of the animations without the need for coding. Games developed in Flash are standalone and could run independently unless it needs to be connected to the database. ActionScript 2 is used to code in Flash because it is easy to understand and develop. Flash is highly secure because the source code is not publicly accessible. MYSQL is used for the database which is a good platform for both basic and advanced projects. PHP connects Flash with MYSQL and enables developers to read, update, add, and remove data.
H. Operating Platform	InfoSecure can run on PC, smartphones, and browsers.
I. Game Evaluation	An advantage of InfoSecure over previously developed games is that every time a topic is played, questions are shuffled to prevent players from memorizing the pattern of correct answers. User progress can be viewed in the player's profile. The user and instructors can view the progress. They can keep track of employee's performance; how many time a topic is played, what are the scores achieved, what information security topics have been more difficult, what are employees' strength and weaknesses. It demonstrates employees' learning curve. Evaluating the recorded information help managers to monitor employees' performance and take necessary actions.
J. Game Achievement	A certificate of accomplishment is rewarded once the full score is achieved for all the topics.

V. INFOSECURE DEVELOPMENT

This section describes the development of the InfoSecure game. InfoSecure enhances previous approaches in a number of dimensions. It offers realism which is the balance between reality and fantasy. Simulation games are favored as they simulate real work environment which allows users to make mistakes and learn from those mistakes without worrying about the consequences of their actions as they would in the real life. The serious game also requires the flexibility and fun appeared in casual games in order to release users' boredom and tiredness.

With the said justification, InfoSecure is developed with a combination of simulation and casual genres. The game is characterized by the strength of simulation and casual genres. InfoSecure consists of eight topics. Every topic addresses one information security policy topic that is selected by HUKM management during semi-structured interviews. The information security topics include 1) phishing, 2) web using, 3) email and spam, 4) malicious code, 5) password protection, 6) privacy and confidentiality, 7) workstation and hacking, and 8) access control.

In order to fulfill the requirement of the simulation genre, hospital theme is used as the main theme of InfoSecure, and medical elements are used in the design of topics. In addition, to fulfill the requirement of the casual genre, each topic is designed differently to avoid boredom and to make the game challenging and fun. Nevertheless, all topics hold the same goal of raising employees' awareness towards information security.

An important advantage of InfoSecure is that the game is dynamic and flexible. As discussed before, the advantage of computer game training is that it can be repeated over time. However, a static game will get boring after repeated a few times. Therefore, to avoid reusing static game and to keep players motivated to participate, InfoSecure is developed dynamically. It allows IT managers to change and customize training content as well as the graphics. For instance, IT managers and instructors are able to change or update information security topics of the game as well as setting the number of questions. It is also possible to change the graphics and the overall look of the homepage and every individual topic. The aim is to keep gameplay more interesting. By changing graphics and content, the game will look fresh in the eyes of the player as if it is a different game. It is also worth noting that such flexibility transforms InfoSecure to a platform that can be used by other healthcare. Moreover, players are able to mute or unmute the background music as they desire.

InfoSecure is developed to satisfy several essential requirements obtained during semi-structured interviews with HUKM decision makers:

- Information security awareness: The overall aim is to design an effective information security awareness training program for HUKM. The training program attempts to raise employees' awareness toward information security and help them adhere to appropriate behaviors that do not compromise the security of information assets and with long-term impact.
- Large coverage: HUKM is categorized as a large organization in which all employees need to be trained toward information security. The advantage of InfoSecure is the capability to cover large population at lower cost.
- Accessibility: InfoSecure is easily accessible. The game will be sent to users via email. Employees receive a link that direct them to the game. This link

redirects users to the game page. It allows the game to run from a web browser without having a huge impact on computing power. Therefore, the game is accessible and runs smoothly even on old computers.

- Content Updatability: IT managers and instructors are able to change or update information security topics of the game as well as setting the number of questions. It is also possible to change the graphics and the overall look of the homepage and every individual topic.
- Fun and motivation: A well-developed serious game is fun, and it promotes employees engagement. InfoSecure is developed with a combination of simulation and casual genres that makes InfoSecure different from previously developed games.
- Performance evaluation: InfoSecure allows IT, managers and instructors, to record and keep track of employees' progress in the game. Instructors can review scores achieved by employees every time they play a topic.
- Repeat: InfoSecure can be played as many times as desired. A successful awareness program never ends and the awareness campaign must repeat its message to the employees. If the message is important, then it should be repeated more often in different manners each time. Since InfoSecure is dynamic, it inhibits higher and active learning with long-term impact.

VI. INFOSECURE INTERFACE

Upon successful login user will be prompt with the welcome page (Figure 3). This page contains brief instruction of the game. By pressing the next button, welcome page disappears and the main page will be entirely visible. Eight linked objects are accessible within the homepage. Each object takes the user to a topic. The user is required to answer all questions correctly for each topic to obtain a full score, otherwise must replay. Once all questions are answered correctly, a green √ icon will appear on top of that particular topic to differentiate a successfully completed topic from others. Once a topic is completed, it will be deactivated and no longer can be played. This helps to push the user to move on and play incomplete topic.

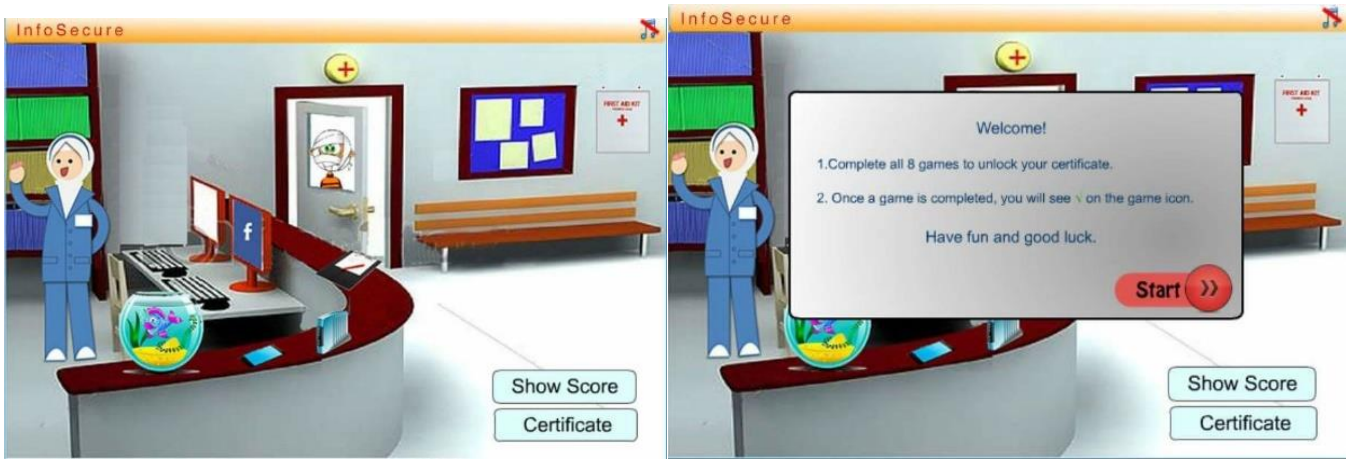

Fig. 3. The Welcome page of InfoSecure

Figure 4 is a screenshot of a game designed to cover a topic on information security, specifically on workstation and hacking. The story of the game is to cure and discharge all patients from the hospital by answering all questions correctly. The number of questions for this topic will be determined between one to ten by the trainer with administrative privilege. There are two icons on the top right corner including mute/unmute and home button. By clicking on the home button user will be redirected to the main page of the game to replay the game or play a different game. Below the top banner, you find a number of 10 beds displayed on the screen, and the number of patients on the beds is according to the number of questions determined by the trainer.

To display a question, the user must click on one of the patients laying on the bed. Once a question is answered correctly, a green color √ appears to confirm that the user has selected the correct answer. Therefore, the patient will be discharged and leave the bed vacant. If the user selects a wrong answer, a red color × appears to indicate that wrong answer is chosen and reveals the correct answer by a green √. Consequently, the patient will remain laying on the bed with a severe headache. After selecting an answer, either correct or wrong, the user can proceed to the next question by clicking on the next question button. All questions must be answered correctly otherwise; user needs to replay the game in order to mark the game as completed on the homepage. The order of questions changes randomly every time the game starts to prevent the user from memorizing the patterns of the correct answer. Once all questions are answered, the result page will come up that shows the topic of the game, the username, and the score.

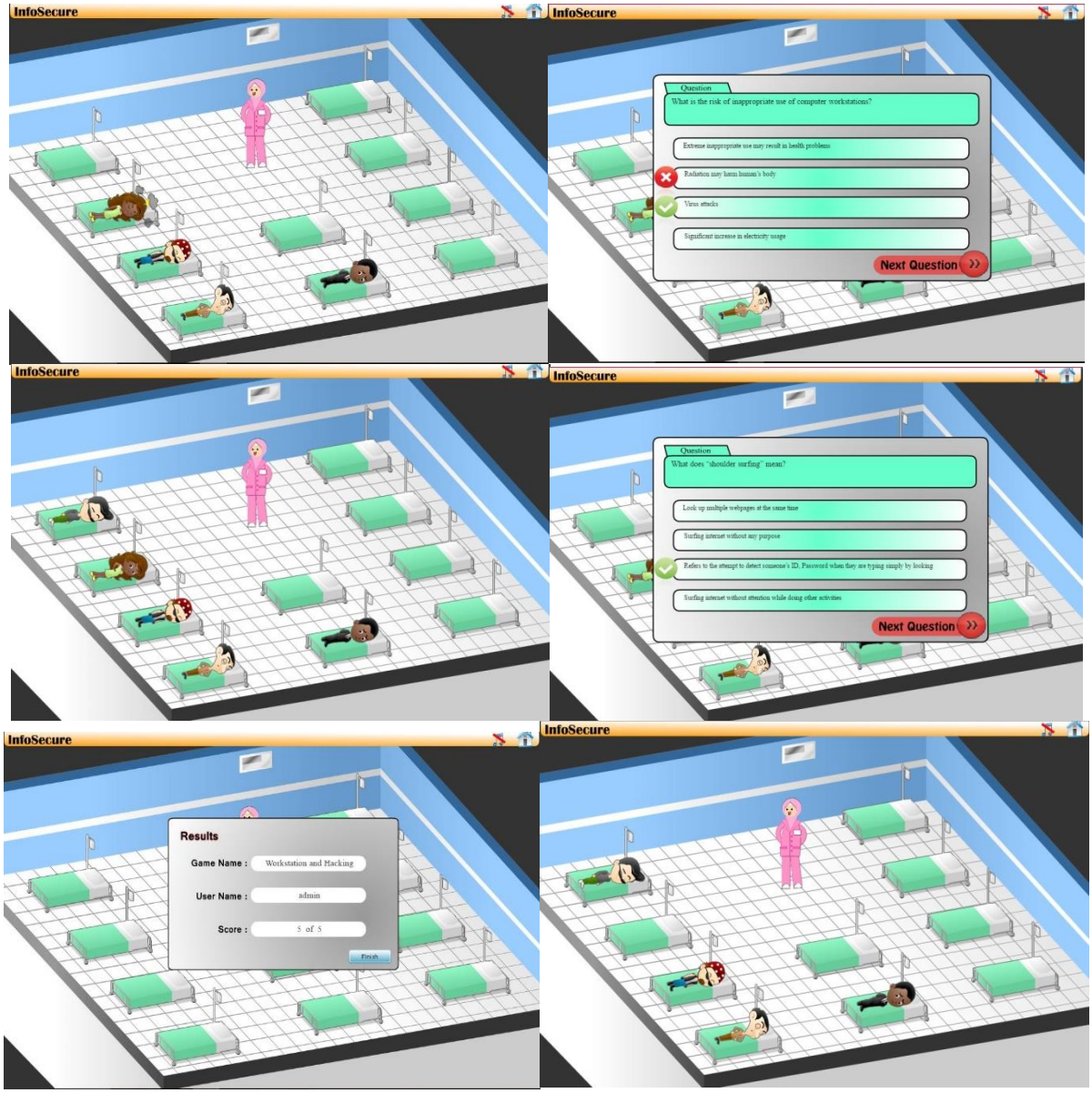

Fig. 4. The InfoSecure workstation and hacking topic

VII. Implementation and Evaluation

Prior to pilot testing, the InfoSecure game was demonstrated for three full professors in computer science specialized in visual informatics, HCI and usability. They provided valuable feedbacks that are incorporated into the game. On the next phase, five students from the faculty of computer science, Universiti Kebangsaan Malaysia, randomly volunteered to play the game. A discussion was held with students and they provided corrective suggestions as well. The actual pilot test was conducted amongst HUKM employees to test the effectiveness and quality of the InfoSecuer game before handing over to IT department to reach out to all employees. A number of five employees randomly volunteered to play the InfoSecure. After playing the game, the participants showed good impressions of the gameplay experience, attraction, the graphics, and its idea.

When users play a topic for the first time, the answer to the information security questions based on their initial knowledge and understanding which might be wrong. Assuming that a player answers two questions correctly and scores 40% when playing a topic for the first time. The player will be prompted with a result page that three questions have been answered wrongly. The player needs to repeat the topic again in order to obtain a full score. In the second attempt, the player should select answers more carefully, knowing previously selected answers were wrong. Now assuming that the player manages to find the correct answer to four questions and scores 80%. There is still one more question, therefore, the player has to start the topic again from the beginning. The player cannot deactivate the topic and mark it as a completed game, before finding the correct answer to all five questions and scores 100%. Therefore, the user has to play the same topic over and over until he finds all the correct answers. Once

the user scores 100% the topic deactivates and is marked as completed.

In order to prevent players from memorizing the sequence and pattern of correct answers, the order of questions changes every time a topic is replayed. That means every time a topic restarts, questions are shuffled to display in random order. The InfoSecure game helps employees gain knowledge on information security and replace it with the wrong information they initially had in their minds. by playing the game, employees understand that they need to think carefully when dealing with electronic health systems. InfoSecure allows users to make mistakes and learn from those mistakes without worrying about the consequences of their actions as they would in the real life.

Every time an employee plays a topic, the scores are recorded in a database; from the first to the last attempt until player scores 100%. User progress can be viewed in the player's profile. The user and instructors can view the progress. They can keep track of employee's performance, the number of times a topic is played, obtained scores, the most challenging information security topics, and employees' strength and weaknesses. It demonstrates employees' learning curve. Evaluating the recorded information help managers to monitor employees' performance and take necessary actions.

A certificate of accomplishment is rewarded to players who scored 100% in all the topics. The certificated could be printed upon completion of the game. Nevertheless, obtaining a 100% score is not the end of the story. It is important to ensure that employees fully understood the topics and integrated them into their daily activities. As a result, the game must be played frequently, decided by hospital management. Therefore, to avoid reusing static game and to keep players motivated to participate, InfoSecure is developed to be dynamic. It allows IT managers to change and customize the training content as well as the graphics. The aim is to keep gameplay more interesting.

The main objective of asking computer science students to play is to get their feedback on the gameplay experience. It is not surprising that computer science students performed well and answered the most question correctly during the first play. However, HUKM employees did not perform well during the first play. They had to play a topic few times until score 100%. Table III shows the employees' records. For instance, the phishing topic was played four times by employee number 3. For the first play, only one question was answered correctly and scores 0%. The second and third play scores are 40% and 80%, respectively. During the fourth play, the player manages to select the correct answers to all questions and scores 100%.

TABLE III. EMPLOYEES' RECORD OF PLAYING INFOSECURE

Topic	**Employee #1**	**Employee #2**	**Employee #3**	**Employee #4**	**Employee #5**
Phishing	1st play: 60% 2nd play: 100%	1st play: 80% 2nd play: 100%	1st play: 20% 2nd play: 40% 3rd play: 80% 4th play: 100%	1st play: 80% 2nd play: 80% 3rd play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%
Web using	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 100%	1st play: 20% 2nd play: 40% 3rd play: 80% 4th play: 80% 5th play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%	1st play: 20% 2nd play: 60% 3rd play: 100%
Email and spam	1st play: 80% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%	1st play: 40% 2nd play: 60% 3rd play: 80% 4th play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 80% 3rd play: 100%
Malicious code	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 100%	1st play: 20% 2nd play: 60% 3rd play: 80% 4th play: 100%	1st play: 40% 2nd play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%
Password protection	1st play: 60% 2nd play: 100%	1st play: 60% 2nd play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%
Privacy and confidentiality	1st play: 20% 2nd play: 80% 3rd play: 100%	1st play: 20% 2nd play: 80% 3rd play: 100%	1st play: 0% 2nd play: 40% 3rd play: 40% 4th play: 80% 5th play: 100%	1st play: 40% 2nd play: 80% 3rd play: 80% 4th play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%
Workstation and hacking	1st play: 20% 2nd play: 80% 3rd play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%	1st play: 0% 2nd play: 40% 3rd play: 60% 4th play: 80% 5th play: 100%	1st play: 20% 2nd play: 40% 3rd play: 80% 4th play: 100%	1st play: 20% 2nd play: 80% 3rd play: 100%
Access control	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 100%	1st play: 0% 2nd play: 40% 3rd play: 80% 4th play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%

The records show that privacy and confidentiality, and workstation and hacking are more challenging topics compare to the others. Employee number 3 did not select any correct answer when played these two topics for the first time and scored 0%. He also scored 0% for the first time playing the topic on access control. Table IV shows employees total plays, the lowest and the highest score on first attempts. The two topics of privacy and confidentiality, and workstation and hacking were replayed more than the other topics, each for a total of 18 times in order to obtain a score of 100%. The lowest first play scores go to privacy and confidentiality (0%), workstation and hacking (0%), and access control (0%). The highest first play score goes to Phishing (80%), email and spam (80%), and access control (80%).

TABLE IV. TOTAL PLAY, LOWEST AND HIGHEST SCORES OF TOPICS

Topic	Total Play	Lowest Score	Highest Score
Phishing	14	20%	80%
Web using	16	20%	60%
Email and spam	15	40%	80%
Malicious code	14	20%	60%
Password protection	13	40%	60%
Privacy and confidentiality	18	0%	40%
Workstation and hacking	18	0%	40%
Access control	14	0%	80%

VIII. INFOSECURE SECOND ROUND PILOT TEST

An awareness training program should not be a one-time session, whereas, it should be a regular program and reinforced periodically. However, many training programs have failed due to users' resistance to participate in the same program. The strength of computer games over other training programs is its capability to be repeated in different time intervals while promoting employees' engagement. InfoSecure is dynamic that allows IT managers to change and customize the training content as well as the graphics. The aim is to keep gameplay more interesting.

HUKM decision makers agreed that the training program should be repeated quarterly. Hence, a post-training program was conducted three months after the initial training. The post-training program aimed to evaluate and measure the success of the InfoSecure game as a training tool. The five employees who participated in the initial training participated in the post-training as well. Table V shows employees' records during the post-training. Looking at employee number 3, then he played Phishing four times during the initial training to score 100%, whereas, during the post-training, he only played the topic three times to score 100%.

TABLE V. EMPLOYEES' RECORD OF PLAYING INFOSECURE

Topic	Employee #1	Employee #2	Employee #3	Employee #4	Employee #5
Phishing	1st play: 100%	1st play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 100%	1st play: 80% 2nd play: 100%
Web using	1st play: 60% 2nd play: 100%	1st play: 100%	1st play: 80% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%	1st play: 80% 2nd play: 100%
Email and spam	1st play: 80% 2nd play: 100%	1st play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%	1st play: 80% 2nd play: 100%
Malicious code	1st play: 40% 2nd play: 100%	1st play: 80% 2nd play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 100%	1st play: 100%
Password protection	1st play: 60% 2nd play: 100%	1st play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%	1st play: 80% 2nd play: 100%	2nd play: 100%
Privacy and confidentiality	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 60% 3rd play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 40% 2nd play: 60% 3rd play: 100%
Workstation and hacking	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%	1st play: 40% 2nd play: 80% 3rd play: 80% 4th play: 100%	1st play: 40% 2nd play: 80% 3rd play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%
Access control	1st play: 80% 2nd play: 100%	1st play: 80% 2nd play: 100%	1st play: 60% 2nd play: 80% 3rd play: 100%	1st play: 80% 2nd play: 100%	1st play: 80% 2nd play: 100%

Similar to the previous records, privacy and confidentiality, and workstation and hacking are more challenging topics compare to the others. However, employees show improvement and obtained better results during the post-training. For instance, employee number 3 who did not select any correct answer for these two topics during initial training, scored 40% for privacy and confidentiality and 40% for workstation and hacking during the post-training. Table VI shows employees total plays, the lowest and the highest score on first attempts. The two topics of privacy and confidentiality, and workstation and hacking were replayed more than the other topics, each for a total of 15 times in order to obtain the score of 100%. Some of the employees scored 100% on the first attempt.

TABLE VI. LOWEST AND HIGHEST SCORES ON FIRST ATTEMPTS

Topic	Total Play	Lowest Score	Highest Score
Phishing	8	40%	100%
Web using	10	60%	100%
Email and spam	10	60%	100%
Malicious code	9	40%	100%
Password protection	9	40%	100%
Privacy and confidentiality	15	40%	60%
Workstation and hacking	15	40%	80%
Access control	11	80%	80%

The result of the post-training showed satisfactory outcome indicating that InfoSecure is an effective tool for the information security awareness training program, not only from the training result but also from the employees' perspective. The objective of this training program was to enhance employees' awareness towards information security. As the results show, there is a significant improvement in employees' performance. Moreover, employees have shown a willingness to participate in the program as they had a pleasant experience during the initial training and enjoyed playing the InfoSecure game.

IX. CONCLUSION

The objective of this paper is to design a serious game for information security awareness training programs for the healthcare industry. To achieve the objective, this paper reviewed the serious game design models and adapted the most effective model. The serious game presented in this paper consists of eight topics; each addressing one information security issue selected by the healthcare IT managers. The topics include phishing, web using, email and spam, malicious code, password protection, privacy and confidentiality, workstation and hacking, and access control. The main advantages of InfoSecure include flexibility, content updatability, and accessibility. Such flexibilities enable organizations to conduct post-trainings without the need to purchase a new game for training. Moreover, not changing the graphics of the game makes it less interesting to play for post-training. Inflexibility in games increases the cost of training, which is a big disadvantage. According to the results, the employees showed good impressions of the game's attraction, graphics, and its idea.

REFERENCE

[1] S. A. Alserri, N. A. M. Zin, and T. S. M. T. Wook, "Gender-based engagement model for designing serious games," in Electrical Engineering and Informatics (ICEEI), 2017 6th International Conference on, 2017, pp. 1–5.

[2] A. Amory, "Game object model version II: a theoretical framework for educational game development," Educ. Technol. Res. Dev., vol. 55, no. 1, pp. 51–77, 2007.

[3] N. A. Bartolome, A. M. Zorrilla, and B. G. Zapirain, "Can game-based therapies be trusted? Is game-based education effective? A systematic review of the Serious Games for health and education," in IEEE Intelligent Systems, 2011, pp. 275–282.

[4] R. C. Basole, D. A. Bodner, and W. B. Rouse, "Healthcare management through organizational simulation," Decis. Support Syst., vol. 55, no. 2, pp. 552–563, 2013.

[5] F. B. García, S. García-Martínez, E. M. Navarrete-Ibañez, and M. J. Cervelló-Donderis, "Designing Serious Games for getting transferable skills in training settings," in Interaction Design and Architecture (s), 2013, no. 19, pp. 47–62.

[6] D. Charles, T. Charles, and M. McNeill, "Using player and world representation techniques from computer games to improve student engagement," in Games and Virtual Worlds for Serious Applications, 2009. VS-GAMES'09. Conference in, 2009, pp. 36–42.

[7] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cybersecurity training and awareness," Comput. Secur., vol. 26, no. 1, pp. 63–72, 2007.

[8] S. De Freitas and M. Oliver, "How can exploratory learning with games and simulations within the curriculum be most effectively evaluated?," Comput. Educ., vol. 46, no. 3, pp. 249–264, 2006.

[9] M. Hu and Y. Kuang, "Human-machine interface: Design principles of pagination navigation in web applications," in Computer Science & Education (ICCSE), 2014 9th International Conference on, 2014, pp. 1140–1143.

[10] W. Hu, "A reusable eduventure game framework," in Transactions on edutainment I, Springer, 2008, pp. 74–85.

[11] T. Monk, J. Van Niekerk, and R. Von Solms, "Concealing the Medicine: Information Security Education through Game Play.," in ISSA, 2009, pp. 467–478.

[12] M. Azwan and B. Ibrahim, "a Certification Criteria for Software of Measuring Instruments Based on Malaysia Environment," 2011.

[13] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on, 2012, pp. 256–262.

[14] H. M. Omar and A. Jaafar, "Usability of educational computer game (Usa_ECG): applying analytic hierarchy process," in International Visual Informatics Conference, 2011, pp. 147–156.

[15] M. Prensky, "J COMPUTER GAMES AND LEARN| NG: D 1 G ITAL GAME-BASED LEARN 1 NG," 2007.

[16] A. Shapi'i and S. Ghulam, "Model for educational game using natural user interface," Int. J. Comput. Games Technol., vol. 2016, 2016.

[17] W. Westera, R. J. Nadolski, H. G. K. Hummel, and I. G. J. H. Wopereis, "Serious games for higher education: a framework for reducing design complexity," J. Comput. Assist. Learn., vol. 24, no. 5, pp. 420–432, 2008.

[18] A. Yusoff, "A conceptual framework for serious games and its validation." University of Southampton, 2010.

[19] N. H. M. Zain, A. Jaafar, and F. H. A. Razak, "SGameFlow framework: how to experience enjoyment in serious game (SG) for motor impaired users (MIU)," in Computer & Information Science (ICCIS), 2012 International Conference on, 2012, vol. 2, pp. 1020–1024.