A Framework for an Effective Information Security Awareness Program in Healthcare

A Case Study of Computer Game in 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*—Electronic Health Record (EHR) is a valuable asset of every healthcare and it needs to be protected. Human errors are recognized as the major information security threats to EHR systems. Employees who interact with EHR systems should be trained about the risks and hazards related to information security. However, there are limited studies regarding the effectiveness of training programs. The aim of this paper is to propose a framework that provides guidelines for healthcare organizations to select an effective information security training delivery method. In addition, this paper proposes a guideline to develop information security content for awareness training programs. Lastly, this study attempts to implement the proposed framework in a selected healthcare for evaluation. Hence, a serious game is developed as a training method to deliver information security content for the selected healthcare. An effective training program raises employees' awareness toward information security with a long-term impact. It helps to gradually change employees' behavior over time by reducing their negligence towards secure utilization of healthcare EHR systems.**

***Keywords*—awareness Training Program; Information Security; Content Development; Electronic Health Record; Human Error; Serious Game**

I. Introduction

There is a wide range of training delivery methods for information security awareness programs. However, research is scant regarding the effectiveness of these methods [1]. The literature shows that many information security awareness training programs have failed to produce long-term impacts on employees' behavior [1][2][6]. The success of any information security awareness program heavily relies on how the content is communicated to its audience [7]. Therefore, it is vital to select the most suitable information security training delivery method [1].

Hence, there is a need to develop a guideline for healthcare organizations to select the most suitable training delivery method for implementation of information security awareness program. It is important to develop a good training delivery method for information security awareness program that is accepted by employees to promote their participation. Furthermore, it is necessary to ensure that information security content is created through a valid process and effectively communicated with employee during awareness training program. Constructing a good information security awareness training program highly relies on the selected delivery method, design of the selected delivery method and training content.

Training Method Selection (TMS) framework is proposed as guideline for healthcare organizations to select an effective training delivery method for information security awareness. The key attributes of effective information security awareness training program are identified to be used in the proposed framework. In addition, the involvement of healthcare decision makers is important to use their insights in order to develop the framework. Hospital University Kebangsaan Malaysia (HUKM) is the selected healthcare for the purpose of this study. A serious game called InfoSecure is developed to test the effectiveness of the TMS framework. In the process of content development, Common mistakes made by healthcare employees were collected through questionnaire and wrong answers were used in development of training content. According to the findings, this study confirms that the selected training delivery method for HUKM produces desirable outcomes and accepted by both organization and employees.

II. Literature Study

The aim of this section is to find the gap and identify issues by understanding the background and previously conducted researches that may lead to potential solutions. There are three fundamental questions to be answered in this section as follow:

The first fundamental question is" how to select effective training method for information security awareness training program?" Health organization faces many challenges when it comes to selecting and effective information security awareness training program. The literature shows most of these programs failed in the past due to different reasons. A guideline is needed to assist organizations in order to select a training delivery method for information security. The Training Method Selection (TMS) is proposed as a solution to assist healthcare organization to select the most suitable information security awareness training delivery method. The TMS framework is influenced by Morrison et al. (2004), Manke and Winkler (2012), and Kissack and Callahan (2010) [17][15][13]. TMS framework is validated by expert panel approach and tested at Hospital University Kebangsaan Malaysia (HUKM) as a selected healthcare for this study.

Based on inputs from HUKM decision makers, computer game is selected as the most suitable information security awareness training delivery method for the organization. However, TMS framework may result different if utilized by other healthcare organization.

To answer the second fundamental question, "How to construct a good training delivery method for information security awareness training program?". A well-designed layout, guideline, conceptual model is needed to construct a successful training program. This model can be formed based on models developed in previous studies. Previous studies recognized serious game as an appropriate solution for information security awareness training program [18][16][6][20]. Although, developing a successful serious game requires a review of adequate guidelines that identified all characteristics to be incorporated in such games. The developed serious game for HUKM is called InfoSecure. The InfoSecure conceptual model is influenced by Yusoff (2010) [24]. InfoSecure is validated by expert panel and pilot test confirms the effectiveness of the game before implementation at HUKM. The main objective of this awareness training program is to raise HUKM employees' knowledge towards information security.

The third fundamental question is "How to develop an information security content for awareness training program?" A guideline is needed to assist organizations to create training content from the sources such as internal policy documents and international standards to be used in the selected training delivery method. Based on previous studies, an information security training content development guideline is proposed to help healthcare organization create information security content to be used as training material. As HUKM information security policy is outdated at the time this research taking place, the policy document is augmented based on information security international standards to be used as reference to create the content. Information security content of this study is validated by expert panel before added into the InfoSecure game. Format of content depends on the selected awareness training method. The result of content development for this study to be used in InfoSecure is 40 multiple choice questions and answers. All forty questions where given to selected number of HUKM employees as open ended questioner in order to collect their common mistakes as collection of wrong answer to be used in InfoSecure.

III. Research Aim

The Effectiveness of an information security awareness program has often been ignored by organizations. Electronic Health records (EHR) are the most valuable assets of every healthcare and it needs to be protected. Human errors are recognized as the major threats to electronic health record systems. Employees who interact with the systems must be trained to understand the risks associated with information security in EHR systems.

There is a wide range of information security awareness techniques. However, research is scant regarding effective information security awareness delivery methods. Although information security training programs can minimize the risks of employees' mistake, the literature shows that many awareness training programs are not effective in raising employees' awareness toward information security. The failure is due to several distinct problems such as lack of employees' willingness to participate. Hence, the main objective of this paper is to provide guidelines for healthcare organizations to implement a successful awareness training program that raises employees' awareness toward information security with a long-term impact.

Training delivery method is the key in designing an effective awareness program for information security. Hence, as the first objective, this study proposes a training method selection (TMS) framework to select an effective training method for information security awareness program. It guides organizations to select the most suitable training delivery method that fulfils organization training needs while promoting employees' engagement and increasing their interest. To meet this objective, semi-structured interviews were conducted at the selected healthcare to obtain insights from decision makers to develop the framework. The TMS framework is implemented in Hospital University Kebangsaan Malaysia as the selected healthcare. Previously conducted awareness training programs at HUKM did not produce desired outcome. Based on the TMS framework, the healthcare decision makers selected computer game method for awareness training program. HUKM requires a fun, creative training programs that covers all employees and can be conducted more frequently. Moreover, it was required that the training program should be organized in a friendly and informal manner and lasts for approximately 30 minutes. In addition, the result shows that the most common information security incident occurring in the organization 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.

As the second objective, this study develops and implements a serious computer game for HUKM to deliver the training content. Serious games are a type of computer games designed for training purposes that bring education and entertainment together. A serious game consists of educational elements with pleasant interface. The developed serious game is called InfoSecure enhances previously developed games in a number of dimensions such as flexibility and fun. The findings indicate that serious games with combination of two genres, simulation and casual, produce satisfactory outcomes. Simulation characteristic of a game 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. Casual characteristic provides flexibility and fun required in serious games. Hence, a combination of the two genres together results in a better serious game.

As the third objective, this study proposes guidelines to develop information security content for awareness training program. Training content must be developed based on i) healthcare internal information security policy, ii) information security international standards, iii) common information security mistakes made by employees, iv) selected training delivery method, and iv) targeted audience profile. It is realized that HUKM internal policy document, in some parts, is not in line with international standards. Therefore, this study proposes policy augmentation for HUKM. Subsequently, training content is developed for HUKM based on the augmented policy document. The main objective of training content is to enforce HUKM information security policy document.

IV. Training Delivery Method Framework

According to Holton (1996), the main failure of training programs is training design [10]. Training delivery method has a direct influence on success of training program [17]. The key to enhance an effective training program is to select an effective training delivery method [17]. In many cases, awareness training seem less likely to enhance employees' performance and they fail to produce satisfactory outcomes [2]. Even though it is necessary to ensure that an information security awareness program covers appropriate topics, it is important to select suitable training delivery methods [1]. Similar to any other programs, the success of an information security awareness program heavily depends on the way awareness information is communicated [7]. There are various types of training delivery methods for information security awareness program adapted by organizations [1]. Even though studies have been carried out to examine the efficiency of training delivery methods, research is scant regarding the effectiveness of the training delivery methods [1]. This study intends to fill this important gap.

The study proposes a training method selection (TMS) framework that helps organizations to select the most effective training delivery method for information security awareness program. The Training Method Selection (TMS) framework is developed based on i) Kemp instructional design model, ii) literature study, and iii) interview at selected healthcare. Kemp' model emphasizes on the importance of training delivery method. In addition, previous studies have identified important attributes that affect the effectiveness of delivery training methods, as discussed in the literature. Moreover, semi-structured interviews are conducted in a selected healthcare to obtain insights from decision makers. Figure 1 present the TMS framework.

A. *Common information security issues*

The first step in designing a training instruction is to identify a problem. Therefore, the initial step to design an information security awareness training program is to identify common information security issues that frequently occur by employees in healthcare organizations. These issues can be found in literature.

B. *Selected information security topics*

Different organizations deal with different information security issues. Therefore, organizations need to identify specific issues to be addressed in awareness training program. Moreover, content sequencing is regarded important as it helps learners understand information and materials easily. Therefore, ordering information security awareness materials by security topics help employees understand the idea properly and effectively.

C. *Training content*

Training content is important to help learners understand information and materials easily. Training content must be developed based on i) organization internal information security policy, ii) information security international standards, iii) common information security mistakes made by employees, iv) selected training delivery method, and iv) targeted audience profile. Organization internal information security policy is an important item to cover in training content [25][26][12]. Addressing internal policy helps employees understand the importance of information security and learn how to prevent incidents from happening. Moreover, looking at employees' common mistake help to determine the level of security awareness training required for organization to avoid over-train or under-train employees [25]. It is important to ensure that employees understand the delivered content; otherwise they may involuntarily put corporate information at jeopardy. Therefore, getting feedback on training content and employees' level of understanding are the keys to confirm personnel comprehension of the content as well as corporate security policy.

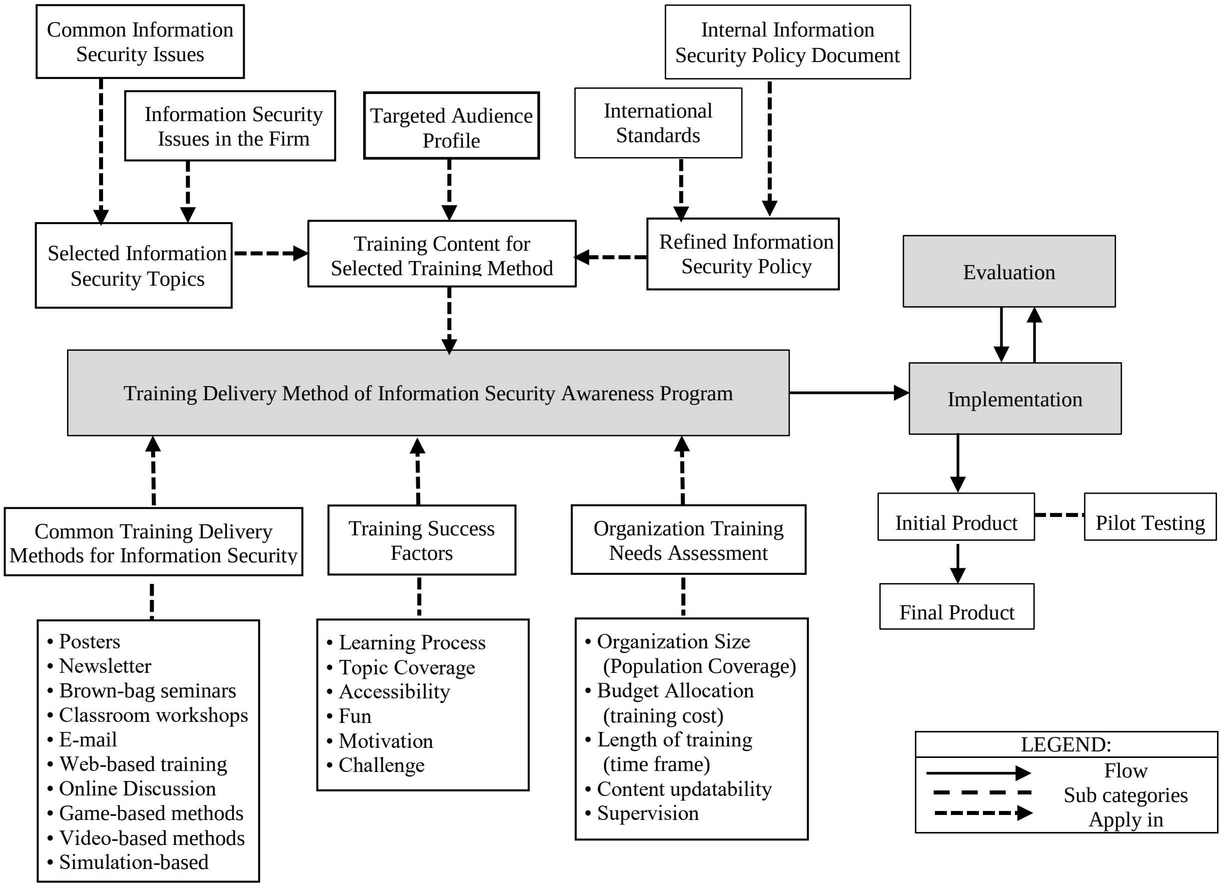

Common Information Security Issues
Information Security Issues in the Firm
Targeted Audience Profile
International Standards
Internal Information Security Policy Document
Selected Information Security Topics
Training Content for Selected Training Method
Refined Information Security Policy
Evaluation
Training Delivery Method of Information Security Awareness Program
Implementation
Common Training Delivery Methods for Information Security
Training Success Factors
Organization Training Needs Assessment
Initial Product
Pilot Testing
Final Product
• Posters
• Newsletter
• Brown-bag seminars
• Classroom workshops
• E-mail
• Web-based training
• Online Discussion
• Game-based methods
• Video-based methods
• Simulation-based
• Learning Process
• Topic Coverage
• Accessibility
• Fun
• Motivation
• Challenge
• Organization Size (Population Coverage)
• Budget Allocation (training cost)
• Length of training (time frame)
• Content updatability
• Supervision
LEGEND:
Flow
Sub categories
Apply in

Fig. 1. Training method selection (TMS) framework

D. *Refined information security policy*

The initial step in developing training content is to identify common information security issues in organization. Next step is to ensure that their internal information security policy document is up-to-date and in line with international standards. Therefore, they need to review and refine the existing internal policy based on the international standards if necessary. Training content development process will be elaborated in details in section X-XI.

E. *Targeted audience profile*

An information security content must be developed taking to account the targeted audience profile. If the massage is deigned too hard to understand, it will drive beginners away and if too easy will make professionals bored. Looking at targeted audience profile help to determine the level of security awareness training required for organization to avoid over-train or under-train employees.

F. *Common training delivery methods for information security*

A critical step in the instructional design process is to select the most appropriate training delivery method. The choice of raining delivery methods has significant impact on individual performance. There are a wide range of training delivery methods. However, reference [1] identified the most proper training delivery methods for information security. The list include i) paper-based (posters and newsletter), ii) instructor-led (brown-bag seminars and classroom workshops), iii) online (e-mail, web-based training, and online discussion), iv) game-based, v) video-based, vi) simulation-based. Narrowing down the list to only those applicable for information security, makes it easier for organization to recognize the most suitable method.

G. *Training success factors*

A well-developed instructional strategy motivates and attracts learners to training information. The training success factors include learning process, topic coverage, accessibility, fun, motivation, and challenge. The key to enhance successful awareness training program is to ensure that the program addresses employees' needs and preferences and it promotes employees' engagement to training activities.

H. *Organization training needs assessment*

The instructional objectives provide a map for designing the instruction and for developing the means to assess learner performance. Therefore, organization training need including population coverage, training cost, time frame, content updatability, and supervision. For instance, organizations may require post-training, hence, content updatability allows trainers to change or edit training content. It is important to ensure that developed instruction solve individual performance.

V. Training Delivery Method Map

To make the TMS framework easy to understand and use, a TMS map (Table 1) is developed that works as a check list for healthcare organizations. Decision makers can select an effective awareness training delivery method based on the TMS map. The left hand side column lists the most proper information security training delivery methods. The rest of the columns are classified into three categories; training success factors, organization training need, training content. Each category consists of several components. If a training method offers a component, it is indicated by **√** mark, if not by × mark.

Decision makers need to carefully select those elements from the TMS map that are most critical to their organization. For example, large population coverage might be very critical to training need of a large organization but less important for small organizations. The training delivery method that has **√** mark for those selected elements is the most suitable method for that organization.

TABLE I. Training Method Selection (TMS) Map

Training Delivery Methods		Training Success Factors						Organization Training Need					Feedback on Content Training
		Active Learning Process	Multiple Topic Coverage	Easily Accessible	Fun	Motivation	Challenge	Large Population Coverage	Low Cost	Flexible Time Frame	Content Updatability	Supervision	Question & Answer
Paper-based Methods	Posters	×	×	×	×	×	×	√	√	√	×	×	×
	Newsletter	×	×	×	×	×	×	√	√	√	×	×	×
Instructor-led methods	Brown-bag seminar	×	×	×	×	√	×	×	√	×	√	√	√
	Classroom workshop	×	√	×	×	×	×	×	√	×	√	√	√
Online methods	E-mail	×	×	√	×	×	×	√	√	√	×	×	×
	Web-based training	√ | ×	√	√	×	×	√ | ×	√	√	√	√	√ | ×	√
	Online Discussion	√	√	√	√	√	√	×	√	×	√	√	√
Game-based method		√	√	√	√	√	√	√	×	√	√ | ×	×	√
Video-based method		×	√	√	×	×	×	√	×	√	×	×	×
Simulation-based method		√	×	×	√	√	√	×	×	×	√	×	√

VI. TMS Framework Validation

An expert panel approach is used to evaluate the TMS framework. Panel of experts is the initial and critical step in establishing content validity. In this study, three professors reviewed the framework and semi-structured interview questions for the purpose of ensuring language, wording, layout, importance of the framework, relevancy of the framework to objectives, process of content creation, clarity of point, topic coverage of the framework and semi-structured interview questions. The expert panel provided the candidate with their inputs, correction and area of improvements.

The expert panel appraisal developed by the researcher is based on (a) literature, (b) requirement of the study, (c) guideline suggested by [14][22]. The panel was asked to provide their recommendations of amendments based on the provided questions. Finally, based on their discussion and comments, the framework and semi-structured interview questions are modified and further improved.

The evaluation confirms the followings: a selected training method based on TMS framework could be the most suitable training method for the selected organization; the selected training method based on TMS framework could promote employees' motivation and participation in training activities; information security content created based on TMS framework could effectively deliver the training content to employees; and the program could successfully enhance employees' knowledge towards information security and strengthens their understanding of organization's information security policy.

VII. TMS Framework Implementation

Hospital Universiti Kebangsaan Malaysia (HUKM) is selected as the case healthcare to implement and evaluate the TMS framework. HUKM has implemented number of awareness training programs that failed to produce satisfactory outcome. The case study approach is now widely used, and there is a growing confidence in its applicability to examine a new finding within real-life context [8][23].

Semi-structure interviews were conducted with key decision makers of the selected hospital. Multiple interviews were conducted with the heads of IT department to identify common issues and mistakes made by employees as well as discussing the training success factor and organization needs assessment. Delphi method is utilized to conduct interviews as it limits the range of respondents' feedbacks and helps coverage toward correct answers. The inputs obtained from the semi-structured interviews intend to evaluate the framework and also to identify which training method is best approach for HUKM. The questionnaire consists of clear and concise instructions divided into four parts.

Eventually, HUKM decision makers converged to the conclusion that computer game-based training is an effective awareness training program to raise employees' awareness toward information security in HUKM. Computer game-based training is perceived as an engaging approach to enhance employees' awareness toward information security. Computer game was selected as it fulfills the organizations' need and promotes employees' engagement.

VIII. SERIOUS GAME

Serious game refers to a game that is primarily designed for training purposes rather than pure entertainment. Computer games designed for training purposes should integrate educational content with multimedia while providing pleasant interface [19]. Reference [4] discussed the educational advantage of 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".

The result of TMS framework revealed that computer game is the most suitable training delivery method for HUKM. Development process needs proper guidelines that comprise all characteristics that should be included in a serious game. Hence, it is important to review available serious game models. This study develops InfoSecure conceptual model based on the model proposed by Yusoff (2010) (Figure 2) as it is the most efficient and effective model for serious games [5]. As Yussof (2010) explains, **capability** is player's capability to be learned in the game. **Instructional content** refers to the subject matter that player is required to learn. Both capability and Instructional content are components of **intended learning outcomes**, which refer to the objective playing a serious game. **Game attributes** are game functions that support players learning and engagement. Game attributes and intended learning outcomes are components of **learning activity**. G**ame genre** refers to style and characteristics a game that specifies the type of environment for the set of activities to be played within the game world. G**ame mechanics** are the components that offer more enjoyment and engagement to a game.

IX. THE INFOSECURE CONCEPTUAL MODEL

Figure 3 is the developed conceptual model for InfoSecure game. Because this is a conceptual model, it can be used as a guideline that visually represents the arrangement of the InfoSecure game elements.

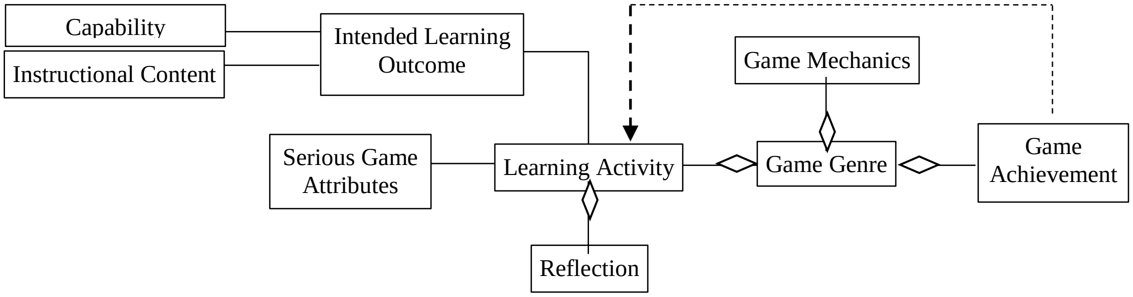


Fig. 2. Yusoff's (2010) serious game model

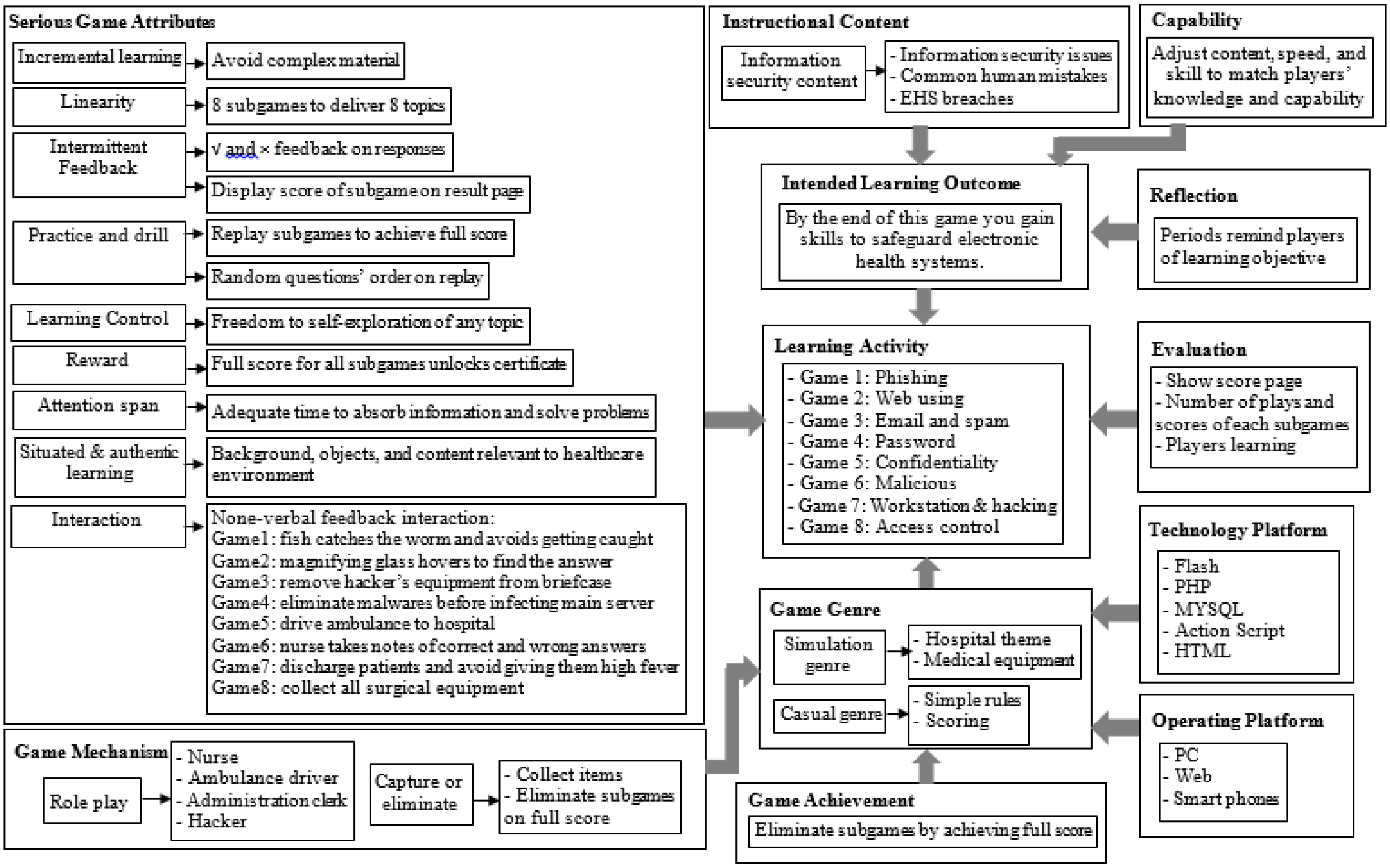

Serious Game Attributes
Incremental learning
Avoid complex material
Linearity
8 subgames to deliver 8 topics
Intermittent Feedback
√ and × feedback on responses
Display score of subgame on result page
Practice and drill
Replay subgames to achieve full score
Random questions' order on replay
Learning Control
Freedom to self-exploration of any topic
Reward
Full score for all subgames unlocks certificate
Attention span
Adequate time to absorb information and solve problems
Situated & authentic learning
Background, objects, and content relevant to healthcare environment
Interaction
None-verbal feedback interaction:
Game1: fish catches the worm and avoids getting caught
Game2: magnifying glass hovers to find the answer
Game3: remove hacker's equipment from briefcase
Game4: eliminate malwares before infecting main server
Game5: drive ambulance to hospital
Game6: nurse takes notes of correct and wrong answers
Game7: discharge patients and avoid giving them high fever
Game8: collect all surgical equipment
Game Mechanism
Role play
- Nurse
- Ambulance driver
- Administration clerk
- Hacker
Capture or eliminate
- Collect items
- Eliminate subgames on full score
Instructional Content
Information security content
- Information security issues
- Common human mistakes
- EHS breaches
Capability
Adjust content, speed, and skill to match players' knowledge and capability
Intended Learning Outcome
By the end of this game you gain skills to safeguard electronic health systems.
Reflection
Periods remind players of learning objective
Learning Activity
- Game 1: Phishing
- Game 2: Web using
- Game 3: Email and spam
- Game 4: Password
- Game 5: Confidentiality
- Game 6: Malicious
- Game 7: Workstation & hacking
- Game 8: Access control
Evaluation
- Show score page
- Number of plays and scores of each subgames
- Players learning
Technology Platform
- Flash
- PHP
- MYSQL
- Action Script
- HTML
Game Genre
Simulation genre
- Hospital theme
- Medical equipment
Casual genre
- Simple rules
- Scoring
Operating Platform
- PC
- Web
- Smart phones
Game Achievement
Eliminate subgames by achieving full score

Fig. 3. InfoSecure conceptual model

X. Policy Augmentation

HUKM has not developed its own information security policy document, and thus, it follows Universiti Kebangsaan Malaysia's (UKM) information security policy. Even though HUKM is ISO certified, there are sections outdated or insufficient in details in the policy. Therefore, to develop appropriate training content, this study augments HUKM information policy document based on relevant international standards. The aim of augmentation is to encourage policy makers in HUKM to update current internal information security policy and to use the augmented document to create future content for post-trainings. To augment HUKM internal policy document, the researcher reviewed and refined the document using international standards including ISO 27002, SANS, and HIPAA.

For demonstration purposes this paper only shows policy augmentation process for "control of logical access" policy. As shown in Table 2, the column on the left is a list of topics selected from HUKM policy document and international standards. The other four columns are selected sources including HUKM, ISO, SANS, HIPAA. The first step is to gather a list of topics. The researchers reviewed HUKM policy as well as the other three sources to identify missing information in HUKM document. For instance, as table shows, HUKM does not have any policy regarding workstation use. The next step is to distinguish which of the topics are covered by each source, as indicated by **√** in the table. Subsequently, the strength and quality of policy statement provided by each source was carefully evaluated in comparison with HUKM's policy statements. Policy statements were extracted from sources and incorporated into HUKM policy document when necessary, as indicated by [**√**].

A. *Control of Logical Access*

The objective is to safeguard healthcare information assets including electronic health record from unauthorized access. Security facilities are required to prevent unauthorized access to health information systems. Logical access to health information systems should be only given to authorized individuals. Table 3 proposes policy augmentation for control of logical access.

TABLE II. POLICY AUGMENTATION

Topics	HUKM	ISO 27002 2005	SANS	HIPAA
Server Security				
Physical Security Control	[√]	√		
Control of Database	[√]	√		
Control of Logical Access	[√]	√		
User Identification	[√]	[√]	√	√
User Authentication	[√]	[√]	[√]	√
Information Back-up	[√]	[√]		
Maintenance	[√]	[√]		
Workstation Use			√	[√]

TABLE III. CONTROL OF LOGICAL ACCESS POLICY AUGMENTATION

HUKM Policy	Augmentation Source: ISO 27002 2005; Sec 11.5.3	Augmentation Source: SANS; Password Policy
User Identification 1. System users are individual or group of users that share the same user account and is responsible for the security of the system used. HUKM identify illegal users through the following steps: a. Given one (1) unique ID to all individual user; b. Store and maintain all user ID responsible for each activity; c. Make sure there is auditing facility to check all user activity; d. Make sure all created user ID is based on application; and e. Changes of user ID for application software must get permission from that Application Systems' Secretariat. 2. HUKM identify inactive user ID are not misused through the following steps: a. Suspend all unused ID facilities for 60 days and delete the ID after the 60 days period, and b. Delete all facilities for users that have moved department or retired; *User Authentication* The system should be able to provide the following facilities: 1. The password entered in the form of not visible; 2. The length of password must be at least eight (8) characters long with combination of characters, numbers or other symbols; 3. The password is encrypted during submission; 4. Password file is kept apart from the data for main application system; and Access attempt is limited to five (5) times only. The user ID must be suspended after five (5) consecutive times of trial	*Password Management System* A password management system should: 1. Enforce the use of individual user IDs and passwords to maintain accountability; 2. Allow users to select and change their own passwords and include a confirmation 3. procedure to allow for input errors; 4. Enforce a choice of quality passwords; 5. Enforce password changes; 6. Force users to change temporary passwords at the first log-on; 7. Maintain a record of previous user passwords and prevent re-use; 8. Not display passwords on the screen when being entered; 9. Store password files separately from application system data; 10. Store and transmit passwords in protected form (e.g. encrypted or hashed) *Password Use* 1. Keep passwords confidential 2. Avoid keeping a record 3. Change passwords whenever there is any indication of possible system or password compromise 4. Select quality passwords with sufficient minimum length 5. Not vulnerable to dictionary attacks 6. Free of consecutive identical, all-numeric or all-alphabetic characters. 7. Change passwords at regular intervals and avoid re-using or cycling old passwords 8. Change temporary passwords at the first log-on 9. Not include passwords in any automated log-on process 10. Not share individual user passwords Not use the same password for business and non-business purposes	*Password Construction Guidelines* All users at HUKM should be aware of how to select strong passwords. Strong passwords have the following characteristics: 1. Contain at least three of the following character classes: a. Lower case characters b. Upper case characters c. Numbers d. Punctuation e. Special characters f. Contain at least fifteen alphanumeric characters. C1. Weak passwords have the following characteristics: a. The password contains less than fifteen characters b. The password is a word found in a dictionary (English or foreign) The password is a common usage word such as: names of family, pets, friends; the words "HUKM, PPUKM"; birthdays and other personal information such as addresses and phone numbers; word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

XI. TRAINING CONTENT FOR HUKM

This section explains the process to create training content for HUKM from the augmented policy document. In what follows, information security questions and answers are described.

A. The Questions

As discussed earlier, the TMS framework was implemented at HUKM and it is found that computer game is the most suitable training delivery method for this healthcare. The purpose of this section, is to develop training content in the form of information security questions. A total of 40 questions are created based on HUKM augmented policy document.

B. The Wrong Answers

This study conducted a survey among healthcare employees to collect employees own wrong answers to information security questions. The wrong answers are, used to design the training content. This approach is helpful i) to understands the knowledge level of employees about security topics, iii) to address employees' real problem in understanding information security topics, and ii) to mislead employees and to evaluate their real understanding of subject matters. For this purpose, information security questions are prepared in form of open-ended structure and they are distributed among employees. For example, many employees responded that the minimum length of strong password is four characters whereas the right answer is eight characters.

C. The Correct Answers

The correct answers, on the other hand, are extracted form HUKM augmented policy document, because the objective of training content is to enforce HUKM policy document. For instance, on user authentication topic, the minimum length of strong password is eight characters as stated in HUKM policy document. However, ISO suggests that a strong password must contain at least fifteen characters. Although HUKM is ISO certified, the correct answer to choose should be minimum of eight characters. However, only few sections of HUKM policy document have insufficient information on some of the selected topics. Therefore, some of the questions and correct answers are taken from international standards and verified by the healthcare. Since HUKM is ISO certified, ISO 27002 is prior to other international standards. Table 4 presents the questions and answers created for password protection.

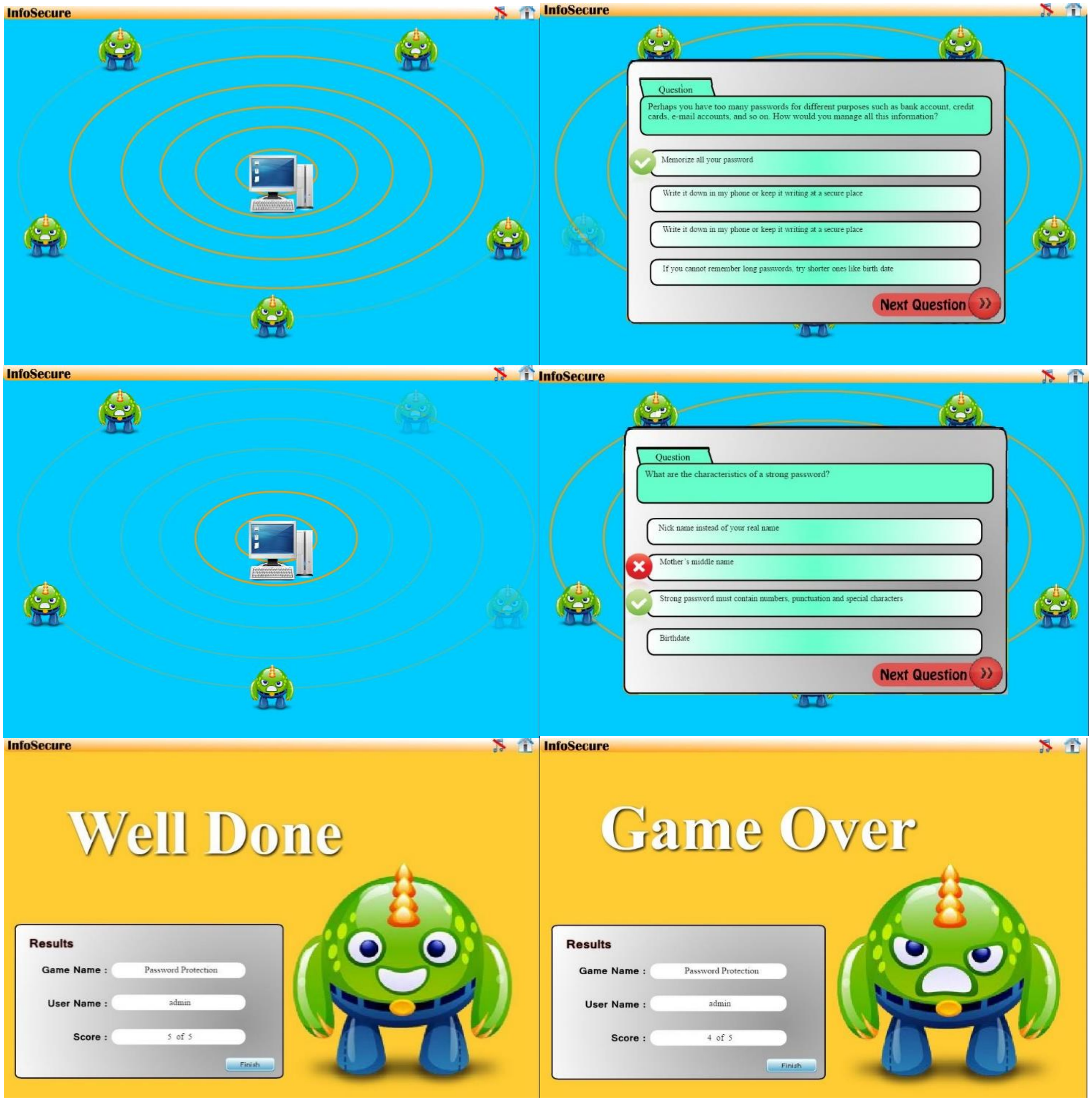
TABLE IV. QUESTIONS AND ANSWERS FOR PASSWORD PROTECTION

Question	Wrong Answer	Correct Answer
Q1. What do you think the minimum length of a strong password should be (e.g. 5 Characters)? S1. HUKM Security Policy 2.3.2 (2)	W1. Four W2. Six W3. Ten	C1. At least eight alphanumeric characters.
Q2. What are the characteristics of a strong password? S1. HUKM Security Policy 2.3.2 (2)	W1. Nick name instead of your real name W2. Mother's middle name W3. Birth date	C1. A strong password contains at least three of the five following character classes: - Lower case characters - Upper case characters - Numbers - Punctuation - Special characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc) - Contain at least eight alphanumeric characters
Q3. What are the characteristics of a weak password? S1. HUKM Security Policy 2.3.2 (2)) S2. SANS; Password Policy (2)	W1. Contains only alphabet and numbers W2. Alphanumerical password W3. Contain at least eight alphanumeric characters password	C1. Weak passwords have the following characteristics: - The password contains less than fifteen characters - The password is a word found in a dictionary (English or foreign) - The password is a common usage word such as: names of family, pets, friends; the words "HUKM, PPUKM"; birthdays and other personal information such as addresses and phone numbers; word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
Q4. Your colleague calls you from home to ask your staff ID and password. What should you do? S1. ISO 27002 2005; Sec 11.5.3 Password Use (1, 2 &10)	W1. Ask for the reason before revealing the password W2. Only reveal the password in case of an emergency and change it afterwards. It is okay if you know the person.	C1. All users should be advised to not share individual user passwords. Do not share HUKM passwords with anyone, including administrative assistants or secretaries.
Q5. Perhaps you have too many passwords for different purposes such as bank account, credit cards, e-mail accounts, and so on. How would you manage all this information? S1. ISO 27002 2005; Sec 11.5.3 (Password Use (1, 2 &10)	W1. Use same password and remember it. W2. If you cannot remember long passwords try shorter ones like birth date. W3. Write it down in my phone or keep it writing at a secure place	C1. Memorize all your password C2. Avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely. C2. Passwords should never be written down or stored on-line without encryption.

Note: Q stands for question; S stands for source; W stands for wrong answer; C stands for correct answer

XII. THE INFOSECURE GAME FOR PASSWORD PROTECTION

This paper develops a serious game called InfoSecure as a training tool to deliver the developed information security content. The InfoSecure game consists of 8 subgames each covering an individual topic. For demonstration, figure 4 shows screenshots of an InfoSecure sub-game that covers password protection. The story of the game is to remove all viruses before reaching the main server by answering all questions correctly. InfoSecure is a dynamic game and not static. That is, instructors are able to change and customize the training content as well as the graphics. Instructors with administrative privilege are able to determine the number of questions from a range of one to ten.



Question

Perhaps you have too many passwords for different purposes such as bank account, credit cards, e-mail accounts, and so on. How would you manage all this information?

✓ Memorize all your password

Write it down in my phone or keep it writing at a secure place

Write it down in my phone or keep it writing at a secure place

If you cannot remember long passwords, try shorter ones like birth date

Question

What are the characteristics of a strong password?

Nick name instead of your real name

× Mother`s middle name

✓ Strong password must contain numbers, punctuation and special characters

Birthdate

Results

Game Name : Password Protection

User Name : admin

Score : 5 of 5

Results

Game Name : Password Protection

User Name : admin

Score : 4 of 5

Fig. 4. Screenshots of password protection game

There are two icons on top right corner: mute/unmute and home button. The home button redirects user to the main page to whether replay the same game or play a different game. Below the top banner, there is a green color dice on upper right side of the screen. Every time user clicks to roll the dice a new question displays and the total number of questions are set to the number of questions determined by trainer. Once a question is answered correctly, a green color ✓ mark appears indicating that correct answer is chosen, and the virus icon fades away. If user selects a wrong answer, a red color × mark appears indicating that user selected a wrong answer, and at the same time, the correct answer will be shown by a green color ✓ mark. Once an answer is select, whether correct or wrong, user can click on next question button and proceed with rest of the questions. User is required to answer all questions correctly otherwise he/she has to replay the game until all questions are answered correctly and the game is marked as completed on the home page. To prevent users from memorizing the patterns of correct answer, the order of questions randomly changes whenever a game starts. Once all questions are answered, a result page appears that displays game topic, username and score.

XIII. InfoSecure Pilot Test

A pilot test was conducted as a preliminary trial for the InfoSecure game. Pilot test helps researchers to identify possible flaws or weaknesses in a product. Ten participants for the pilot study, who volunteered to play the InfoSecure game, were randomly selected and divided into two groups. Five multimedia students from UKM made up the first group, while another twenty HUKM employees made up the second group.

Users who play a subgame for the first time would answer information security questions based on their initial knowledge and understanding, which may be incorrect. A player who answers two questions correctly and scores 40% when playing a subgame for the first time would know that he has answered three questions incorrectly. The player then has to repeat the subgame. In the second attempt, the player would be more cautious in answering the questions, having known that some of the previously selected answers had been incorrect.

With the assumption that the player manages to answer four questions correctly and scores 80%, he still has one question to answer, and thus has to play the subgame all over again. The subgame cannot be deactivated and marked as completed until all five questions have been correctly answered and a 100% score is attained. Hence, the subgame has to be replayed until all of the questions are correctly answered. Once the 100% score is attained, the subgame will deactivate and will be marked as completed. The order of the questions changes every time the subgame is replayed so that a player is prevented from memorizing the sequence and pattern of the correct answers. This is achieved by shuffling the questions so that they are displayed in a random order every time the subgame restarts.

Employees gain two benefits by playing the InfoSecure game; it helps them to gain knowledge on information security, and to replace the incorrect information they might initially have in their minds prior to playing the game. It also helps them to understand the importance of thinking carefully when dealing with the electronic health systems. In the game, users are allowed to make mistakes and learn from them without having to worry about the consequences of their actions as they would in real life.

A player's (employee) score for each subgame, which includes his very first attempt until his last attempt in attaining the 100% score, would be recorded in a database. User progress is displayed in the player's profile, which can be viewed by both the player and the instructors. This helps the instructors to keep track of the employees' performance which demonstrates their learning curve. The aspects of player performance include the frequency of a subgame being played, the scores attained, the most difficult information security topics, and also the employees' strengths and weaknesses. The ability to evaluate the recorded information helps managers in monitoring their employees' performance and in taking the necessary actions. Players who scored 100% in all the subgames will be awarded with a certificate of accomplishment, which can be printed once the game is completed.

Nevertheless, obtaining 100% score is not the ultimate goal since it is crucial for the employees to fully understand the topics and to integrate them in their daily activities. Therefore, the game must be played frequently, as determined by the hospital management. In line with the aim of keeping the gameplay more interesting, and to avoid the reuse of static games and to maintain the players' motivation in taking part in the game, InfoSecure is developed to be dynamic by allowing IT managers to change and customize the training content as well as the graphics.

Getting the feedback on gameplay experience is the key objective in asking computer science students to participate in the game. It is not surprising that even during the first play of the game, the computer science students have managed to perform well by answering most of the questions correctly. HUKM employees on the contrary, had to play a subgame a few times before scoring 100%. Table 5 below shows sample of five employees' records for subgame covering password protection topic. Employee number 3 for example, played the phishing subgame four times. For the first play, he managed to score only 20% by getting one correct answer. For the second and third plays, the score had increased to 40% and 80% respectively. During the fourth play, the player managed to select the correct answers for all the questions and thus scored 100%.

TABLE V. EMPLOYEES' RECORD OF PLAYING INFOSECURE

Subgame	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%

The record shows that privacy and confidentiality, and workstation and hacking are the most challenging topics compared to other topics. The score of employee number three were both 0% when he played the above two games for the first time since none of his answers were correct. His score was also 0% when he first played the subgame on access control. Employees' total plays and their lowest and highest scores on their first attempt are shown in Table 6. The two subgames of privacy and confidentiality, and workstation and hacking were replayed more than the other subgames, each for a total of 18 times in order for the players to obtain a score of 100%. The lowest first play score goes 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 VI. LOWEST AND HIGHEST SCORES ON FIRST ATTEMPTS

Subgame	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%

XIV. CONCLUSION

This research is a noteworthy attempt to address the issues concerning the effectiveness of information security awareness training programs. The research findings revealed the importance of training delivery method and training content in designing an effective information security awareness training program. Moreover, it is found that previously designed training programs failed because they were neither supported by organizations' needs nor accepted by employees. The findings in this study show that an effective information security awareness training program should be designed based on organizations' training needs while promoting employees' engagement and increase their interest.

Therefore, it is vital to give considerable attention to develop training delivery method and training content. Hence, this study proposed a training method selection (TMS) framework that helps organization to select an effective training delivery method for information security awareness program. The framework is based on the key attributes of effective training delivery method include training success factors and organization training needs. The selected training method based on the TMS framework is both supported by organization and accepted by employees.

By using the augmented information security document as the training content, and the computer game as the training tool, policy content was effectively delivered to employees to enhance their awareness. The result of this study reflects in enhancing employees' awareness toward the augmented information security policy in HUKM. An interactive computer game-based awareness training program gradually reduces employees' negligence and promotes the secure utilization of EHR system in HUKM to protect electronic health records.

Measuring employees' level of understanding of information security before and after the awareness training program indicates that the implemented program provides desired outcome. Employees have acquired better understanding of information security and they can manage to handle security matters in a way that limits damage and reduces recovery time and costs. The training program must be repeated frequently to keep employees updated and to change their habits over time. The success of the training program at HUKM shows that TMS framework is effective and it can be used as a guideline to select an effective training delivery method. Nevertheless, the TMS framework can be used by any healthcare to select, design and implement a successful information security awareness training program.

XV. RECOMMENDATION FOR FUTURE STUDIES

There is a wide range of information security awareness techniques. However, research is scant regarding effective information security awareness delivery methods. It is necessary for counselors, educators, and professionals to consider the findings obtained from the current study to further enhance awareness training programs. The findings can be used as a resource material for researchers, scientists, and university authorities who wish to conduct research in the same field. Therefore, the findings will help as supplementary evidence to obtain new results.

This study investigated a wide range of concepts to enhance effectiveness of information security awareness training program. Even though the findings of this study contribute to the field of information security, a few recommendations have yet to be provided for future research. Considering the depth and complexity of the topic there is room to explore and investigate more. Future researchers are recommended to study more elements affecting effectiveness of awareness training programs. Moreover, the findings of this study are limited to healthcare sector and are not generalizable to all organizations, Future studies are recommended to yield more representative active results.

REFERENCE

[1] Abawajy, J. 2012. User preference of cyber security awareness delivery methods. *Behavior & Information Technology* 33(3): 237–248.

[2] Annetta L.A. 2010. The "I's" Have It: A Framework for Educational Game Design. *Review of General Psychology* 14(2): 105-112.

[3] Apperley, T.H. 2006. Genre and Game Studies: toward a Critical Approach to Video Game Genres. *Simulation & Gaming*, 37(1).

[4] Bartolome, N.A., Zorrilla, A.M., Zapirain, B.G. 2011. Can game-based therapies be trusted? Is game-based education effective? A systematic review of the serious games for health and education. *The 16th International Conference on Computer Games*. University of Deusto.Avda. Universidades, Spain, 275-282.

[5] Buendía-García, F., García-Martínez, S., Navarrete-Ibañez, E.M. & Cervelló-Donderis, M.G. 2013. Designing serious games for getting transferable skills in training settings. *Interaction Design and Architecture(s) Journal* (19): 47-62.

[6] Cone, B.D., Irvine, C.E., Thompson, M.F., Nguyen, T.D. 2007. A Video game for cyber security training and awareness. *Computers & Security* 26: 63-72.

[7] Gardner, B., & Thomas, V. 2014. Building an information security awareness program: defending against social engineering and technical threats. *Elsevier*.

[8] Hartley, Jean. (2004). Case study research. In Catherine Cassell & Gillian Symon (Eds.), Essential guide to qualitative methods in organizational research, 323-333. London: Sage.

[9] HIPAA (The Health Insurance Portability and Accountability). 2014. www.hhs.gov/hipaa [10 January 2014].

[10] Holton, E. F. 1996. The flawed four level evaluation model. *Human resource development quarterly 7*(1): 5-21.

[11] ISO (International Organization for Standrdization) 27002. 2005. Standards. http://www.iso.org/iso/home/standards [23 February 2014]

[12] Johnson, E. C. 2006. Security awareness: switch to a better programme. *Network Security* 2: 15-18.

[13] Kissack H. C., Callahan J. L. 2010. The Reciprocal influence of organizational culture and training and development programs: building the case for a culture analysis within program planning. *Journal of European Industrial Training*, 34(4): 265-380.

[14] Iarossi, G. (2006). The power of survey design: A user's guide for managing surveys, interpreting results, and influencing respondents: World Bank Publications.

[15] Manke, S., Winker, I. 2012. The habits of highly effective security awareness program: A cross-computer comparison. *Internet Security Advisors Group*.

[16] Monk, T., Niekerk, J. & Solms R. 2010. Concealing the medicine: information security education through game play. *Institute for ICT Advancement, Nelson Mandela Metropolitan University*.

[17] Morrison, G. R., Ross, S. M., Kemp, J. E., & Kalman, H. (2004). *Designing Effective Instruction*: John Wiley & Sons.

[18] Nagarajan, A., Allbeck, J.M. & Sood, A. 2012. Exploring game design for cybersecurity training. *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Bangkok, Thailand*.

[19] Omar, H.M. & Jaafar, A. 2011. Usability of educational computer game (Usa_ECG): applying analytic hierarchy process. *International Visual Informatics Conference*,147-156.

[20] Prensky, M. 2001. True believers: digital game-based learning in the military. *From Digital Game-Based Learning, McGraw-Hill*, 2001.

[21] SANS (The System Administration, Networking, and Security, https://www.sans.org [22 May 2014].

[22] TrainingCheck. 2015. How can I pilot test the evaluation design and settings? http://www.trainingcheck.com/help-centre-2/faqs/evaluation-design-and-management/how-can-i-pilot-test-the-evaluation-design-and-settings/ [2 December 2015].

[23] Yin, R. K. (2003). Case study research: Design and methods. Sage Publications, Inc, 5, 11.

[24] Yusoff, A. 2010. A Conceptual Framework for Serious Games and its Validation. Thesis for the degree of Doctor of Philosophy. School Of Electronics and Computer Science, University 0f Southampton, United Kingdom.

[25] Security Standard Council. 2014. Information Supplement: Best Practices for Implementing a Security Awareness Program.

[26] Yanus R., &Shin. N. 2007. Critical success factors for mapping an information security awareness program. Proceedings of the Sixth Annual ISOneWorld Conference, Las Vegas, Nevada.