Awareness Training Transfer and Information Security Content Development for Healthcare Industry

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) becomes increasingly pervasive and the need to safeguard EHR becomes more vital for healthcare organizations. Human error is known as the biggest threat to information security in Electronic Health Systems that can be minimized through awareness training programs. There are various techniques available for awareness of information security. However, research is scant regarding effective information security awareness delivery methods. It is essential that effective awareness training delivery method is selected, designed, and executed to ensure the appropriate protection of organizational assets. This study adapts Holton's transfer of training model to develop a framework for effective information security awareness training program. The framework provides guidelines for organizations to select an effective delivery method based on the organizations' needs and success factor, and to create information security content from a selected healthcare's internal information security policy and related international standards. Organizations should make continual efforts to ensure that content of policy is effectively communicated to the employees.**

Keywords*—information security; human error; awareness training program; training content; security policy; electronic health record

I. Introduction

The general objective of this paper is to enhance effectiveness of information security awareness training programs. More specifically, this paper aims to develop a framework that works as a guideline for organizations to select the right training delivery method that produces desirable outcomes. An effective training method must fulfil organization's needs and requirements while taking into account employees preferences. The paper also offers recommendations on how to augment internal information security policy document in healthcare sectors.

This study is influenced by importance of personal data protection to encourage researchers to study factors influencing users' behavior and attitudes toward information security, which impacts integrity of healthcare organizations. Security breaches are inevitable threats that always challenges organizations distinctively. Thus, organizations need to safeguard vital information and assets to prevent organization's integrity from being compromise. Information security breaches result in both direct cost (e.g. loss of intellectual property) and indirect cost (e.g. loses of reputation and potential loss in market share).

Human error is considered as the biggest threat to information security effectiveness [3]. Lack of employees' attention to security policy and standards is the real threat to information system. According to IT security practitioners survey conducted by [17], minimum of 78% of security breaches experienced by organizations are as a result of employees' negligence (Fig 1). Nevertheless, human error can be minimized through awareness training programs [4]. The significance of information security is best defined as the level of user comprehension on Information security awareness. In every organization, employees have varying knowledge of information security awareness [20].

Human errors are categorized into normal human errors and abnormal human errors. Normal human errors refer to individual honest mistakes that are already recognized and can be prevented in advance [5]. These kind of errors can be corrected through training programs with an intention to promote behaviors of individuals toward organizational policy. Education and training programs in organizations can help to improve employees' awareness toward security of e-health system and help them to adhere to appropriate behaviors that do not compromise the security of the system.

In what follows, the background of the study is presented. Section three illustrates the research design. The conceptual framework is presented in section four of this paper. Section five and six discus training content and information security document, respectively. Section seven focuses on training delivery methods. Conclusion is the last section of the paper.

II. Background

Even though the number of information security awareness training programs are growing progressively, there is inadequate evidence to verify their effectiveness and impact on daily activities in a work environment [21]. Literature [6][13] has stated that some of the information security awareness training programs are not effective enough. For instance, number of awareness training programs tends to be more informative without integrating into employees' daily activities that leads to disciplinary actions. Some other awareness training programs are only provided as one-time session that cannot truly change users' behavior toward information system. Awareness training programs should be a regular activity and reinforced periodically.

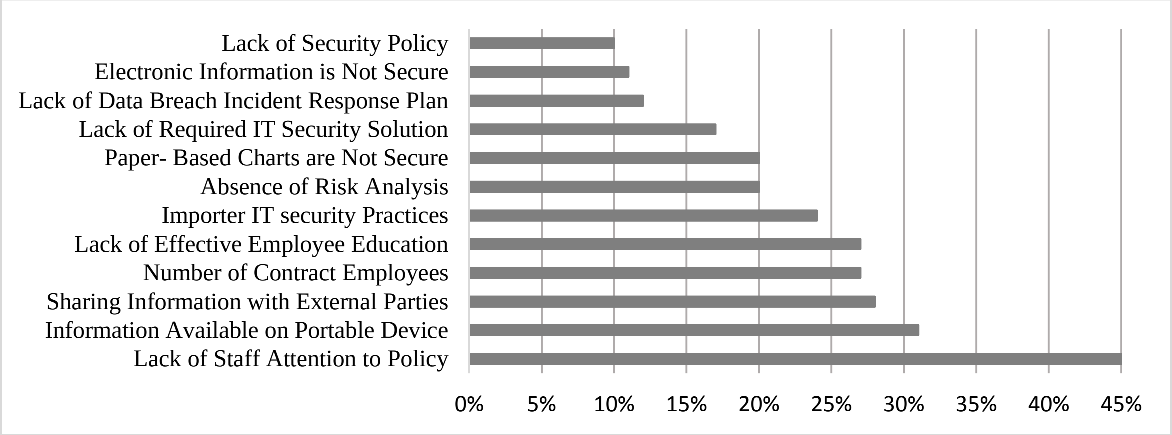

Fig. 1. Factor that Mostly Put Data at Risk

Source: [17]

Training and awareness programs are an effective approach to reduce the risk of individual contribution in electronic health system. However, routine, traditional training programs have been failed because they do not involve critical thinking and do not require users to think about security concepts [19]. On the other hand, there are new interactive training approaches that have been successful to engage employees with training activities including computer games, web-based sessions, E-learning, teleconferencing, and crossword puzzles. The key to impart a concept is to hold users engaged sufficiently long so he or she will absorb that concept, especially when the training program is mandatory.

Another reason for awareness training failure is some of training programs are too advanced for trainees. Employees, particularly those with no advance computer skills such as ordinary staff working in healthcare clinics, have different level of computer knowledge, and thus they require to be trained differently. It was also observed that most of trained employees do not attempt to apply the learned skills in work environment [6][13]. Moreover, many awareness training programs do not measure users' performance before and after the training, and therefore, it is not possible to evaluate the training's outcome. Additionally, number of employees are not motivated to contribute in awareness training program as the program do not promote creative activates [14]. Similarly, [19] argued that traditional and routine information security awareness training programs have been failed because they do not involve critical thinking and do not reinforce users to think about security concepts.

Effective awareness training techniques should be differentiated from ineffective ones [15]. Literature [21] stated that it is essential to increase the effectiveness of information security awareness training programs by encouraging employees to make effort in transferring the skills learned to their daily job activities. It is important to understand and emphasize the factors that differentiate effective trainings from ineffective trainings. Consequently, the existing gap of information security awareness training programs should be bridged to refine and improve the effectiveness of training programs [16][9].

Furthermore, Content of information security awareness training program should be developed from organization's policy based on the selected training technique. Each training approach requires specific content structure to be fitted in the program. The main objective of training content is to enforce information security policy document. Professional and complicated training material makes employees confused or bored towards subject matters. Hence, the training content should be easy to comprehend to motivate the trainees to learn as well as ensuring the delivery of selected content. Exceptionally, in the domain of information security, developers of most training programs are the experts who do not take audience's profiles into account.

III. Research Design

Training is ineffective unless translated into individual performance [23]. Effectiveness of information security awareness is often an overlooked element of an organization's security program. There is a broad range of awareness training delivery methods. However, research is insufficient regarding the effectiveness of delivery methods [1]. Similarly, a side-by-side comparison of different awareness delivery methods of information security is lacking [1][6]. Training programs can truly make a difference in employees' performance, and hence, it is important to understand effective transfer of training in organizations.

The aim of this research is, firstly, to develop a conceptual framework for effective transfer of training, and an opt-in framework for selecting an effective awareness training delivery method. Secondly, to provide a side-by-side comparison of different information security awareness delivery method. This guideline will help organizations to effectively select a delivery method and design a training program based on the organizations' needs and success factors. Lastly, to offer insights on augmentation of internal information security policy document to be used by healthcare organizations.

Hospital Universiti Kebangsaan Malaysia (HUKM) is one of the leading healthcare organizations in Malaysia that has adopted electronic healthcare systems. HUKM is selected as primary healthcare to collect necessary information to conduct this study. A series of semi-structured interviewees were conducted with HUKM decision makers in order to obtain necessary information to design the framework. The collected data is significant to create information security content for the selected healthcare and vital in the process of developing the framework. The framework can be used as a guideline to adapt an effective technique for information security awareness training programs. This guideline will be used to help decision makers to measure strength and weaknesses of each awareness training technique with respect to the organization's need. The developed framework can be used by any organization to select a successful awareness training program.

Even though HUKM is ISO certified, nevertheless, there are insufficient details or outdated sections in the internal information security policy document. To create appropriate information security content for awareness training program at HUKM, this study attempts to augment hospital's internal information policy document based on relevant international policies, as explained in next sections. The purpose of augmentation is to encourage HUKM's policy makers to update their internal information security policy. However, it shows the process of content creation to be followed by other healthcare organizations to enhance their internal security policy document. This is an inevitable stage before creating content or selecting a proper awareness training technique.

A. *Transfer of Training*

Holton (1996) developed a training conceptual model that focuses on individual performance. Learning, individual performance, and organizational results are three primary outcomes of the model for training intervention. These outcomes are described, respectively, as the learning outcome achievement desired by an organization, learning being applied on the job as a result of change in individual performance, and results at the organizational level as a consequence of change in individual performance. Fig 2 demonstrates the Holton's transfer of training model. Holton's model suggests that transfer of training is affected by three crucial factors including motivation to transfer, transfer climate, and transfer design. Only when the three primary influences on transfer behavior are at their appropriate levels, learning is expected to lead to change individual performance [9].

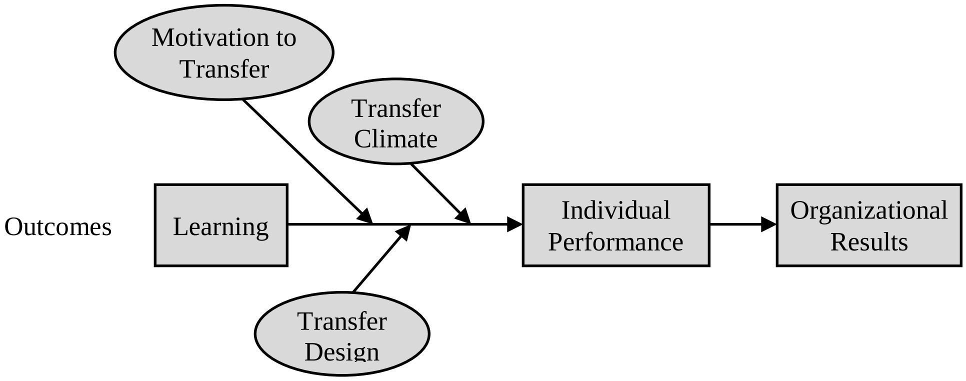

Fig. 2. Holton's Factors Affecting Transfer of Training, (1996)

IV. Conceptual Framework

The conceptual framework of this study is influenced by Holton's model (1996) (Fig 3). New components are added to enhance the pre-existing model. Holton proposes motivation to transfer, transfer design, and transfer climate as three major components of transfer of training that directly influence individuals' performance. This paper suggests that primarily effect of these components is on the choice of training delivery method [9]. Holton stated that learning is expected to lead to individual performance change. However, this study argues that the impact of learning on individuals' performance is affected by training delivery method. Therefore, it is important to put extra attention in selecting an effective method, especially when it comes to information security. Rapid changes, new trends, and security concerns requires constant update of learning outcomes. Demand for awareness is increasing every day and new training methods are introduced and utilized by organizations. If awareness training is effective, then it will significantly enhance individuals' performance. Hence, it is important to select an effective awareness training method that can fulfill organizations' need and requirements. It is also vital to consider training success factors and organizations' culture in order to succeed.

Holton stated that for training program to yield organizations results, it should have the ability to achieve results and motivate the organization and individuals to practice. Again, when it comes to motivation, training method plays a significant role. Effective training methods promote individual willingness not only to participate in training program but also to apply lesson learnt in their daily tasks. Moreover, Information security awareness training program is not a onetime task and it needs to be repeated frequently in order to improve the result and measure its effectiveness in enhancing employees' awareness. The aim of awareness training programs is to better safeguard organizations' assets and information security infrastructure.

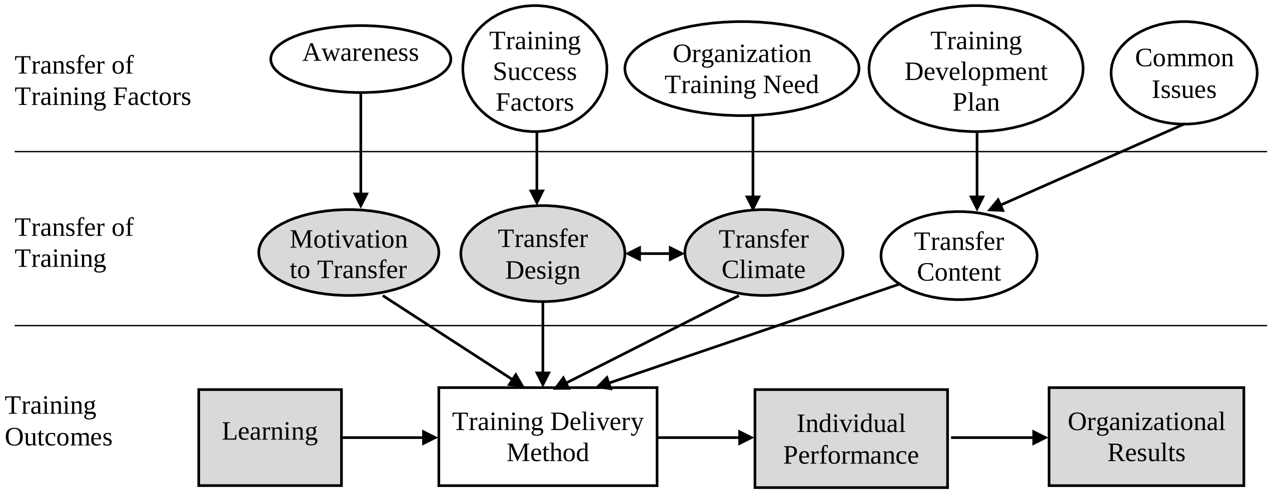

Fig. 3. Factors Affecting Transfer of Information Security Awareness Training Program

A. *Motivation to Transfer*

Hilton defined Motivation to transfer as individual's desire to transfer the necessary knowledge and skills in the training program on the job. This paper argues that awareness can motivate employees to learning. Employees are not aware of their roles to mitigate security issues. Survey conducted by [17] titled *Human Factor in Data Protection* revealed that most of risks in security breaches are driven from a lack of attention by staff to the security policy of an organization. Employees need to be aware of their important role in protecting organization's vital information to avoid compromising the system by rookie mistakes. Understanding the importance of their role in security effectiveness will motivate employees to attend training programs and incorporate their learning into their job performance.

B. *Transfer Climate*

The transfer climate arises from employees' perception of their work environment. It influences the degree in which employees apply the learned skills on the job. Holton defined transfer climate as a mediating variable in the relationship between the organizational context and employees' job attitudes and work behavior. Similarly, an effective awareness program must be based on the characteristics of an organization including organization size, business requirement, budget, target audience, and organization mission and culture. A properly designed awareness program that is in line with organization's need will effectively influence employees' attitude and work behavior.

It is crucial to constantly enhance the information security awareness culture in organizations and transform this culture into actual behavior. One way to improve training climate is to distinguish how different organizations have different needs. A more efficient and cost effective approach to implementing an employee security awareness model is to use a specific program that addresses the specific needs of the organization. Awareness programs must be designed with intention of creating organizational-wide security-minded cultures so that people work in a more secure manner and protect the assets of their organization [1].

C. *Transfer Design*

Holton's model did not provide guidelines to explain what constitutes appropriate transfer designs. According to Holton, the main failure to transfer is training design. In the context of information security, there are various types of security awareness delivery methods adapted by organizations. However, as stated by [2][6], many programs are not effective enough to change employees' attitude and work behavior. Awareness programs often seem less likely to improve employees' performance and many programs fail to enhance expected outcomes. The training itself has a direct influence on transfer of training and the key is to design an effective awareness program. Even though there are some researches on the efficiency of various information security delivery methods, but research is scant regarding effective delivery method of information security awareness.

This study provides guidelines for organizations on how to decide on an effective awareness delivery method for their organization. Enhancing an effective awareness program requires decision makers to make critical decisions about training delivery method as well as *training success factors*. Although it is important for a security awareness program to ensure that the appropriate topics are covered, it is vital to select the right delivery methods [20]. As with any program, the success of information security awareness program will rely heavily on how the awareness information is delivered [1]. As stated by [7], "*The lecture as a teaching tool is dead. Current programs don't work because we rely on old models of teaching. People learn in different ways. Some people are visual learners, while others learn better from reading or discussing. We need to move away from canned* web-*delivered training to interactive, hands-on learning to build more effective security awareness programs*" [7].

D. *Transfer Content*

This study suggests transfer content to be the fourth factor in transfer of training in Holton's model. Holton stated that the three crucial factors affect transfer of training are motivation to transfer, transfer climate, and transfer design. However, the importance of training content in selecting an effective delivery method is disregarded. Training content must fit to the selected delivery method. The structure of content affects the choice of delivery method. The approach by which content is presented will affect the choice of delivery method and, consequently, it affects individuals' performance. For instance, MCQ structure cannot be delivered in conference or brown bag seminars, instead web-based training or computer game-based training are proper choice for MCQ structure.

Holton stated “trainer judge training content to reflect job requirement'. It is essential to pointing out that training content must fit targeted users as well. Content must be relevant and user specific. Different users with different background require different approaches. Many training programs fail due to the complexity or inadequacy of the training materials. For instance, Training programs with too professional and complicated contents make employees bored and confused. There must a development plan to create proper content for targeted audience.

Literature [8] proposed guidelines for healthcare organizations to develop information security training content. As stated by the authors, the content of an information security awareness training program must be driven from organization information security policy.

V. Training Content

As a preliminary step, organizations should identify the information security mistakes commonly made by employees to be used in developing training content. In other words, training content should cover common mistakes occurring in organization. Moreover, training content should be tailor made to organizations' internal information security policy while consistent with international standards [18]. It is also important to note that information security mistakes made by junior employees may be different from those made by senior employees. Therefore, training content should cover all target employees with different level of awareness knowledge [4].

VI. Information Security Policy Document

There is no specific information security policy document tailored for Hospital Universiti Kebangsaan Malaysia (HUKM), therefore, they operate on Universiti Kebangsaan Malaysia (UKM) security policy document. However, once comparing with international standards, it was recognized that the information security policy document is outdated and it needs to be augmented. Hence, new policies are proposed to augment the current information security policy document (Table 1). The international standards consider for augmentation of HUKM information security policy document include:

- *ISO 27002* which provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment.
- *SANS* (The System Administration, Networking, and Security) institute, which provides information security policy and standards as a guideline for organizations to develop and implement security policies.
- *HIPAA* (The Health Insurance Portability and Accountability Act of 1996) that is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission.

Table 1 demonstrates overview of steps were involved in augmenting the HUKM's information security policy document. First, HUKM's information security policy topics were acknowledged among the three international sources to identify relevant clauses and controls (specified by **√**). Second, strength and quality of policy statement provided by each source is evaluated, and then, compared them with HUKM's policy statements. Next, indispensable information were extracted from the sources (specified by bracket) to be added to relevant part of policy document. Supplementary sections are proposed when required to enhance HUKM's policy document. As shown in the table below, two sections have been added to the augmented document and existing sections were updated in comparison with other relevant international standards.

VII. Training Delivery Method

As mentioned earlier, there are number of awareness training delivery methods. Organizations need to select an effective training delivery method based that can fulfill training needs of both organization and employees. Selection of a training method should be based on the information obtained from interviews with management and the pre-developed training program plan. The selected technique should fulfill the need of both organization and employees.

A guide to selection of awareness training program framework (Fig 4) and selection of awareness training program guidelines (Table 3) aim to provide a guideline for decision makers to select an effective awareness training method to deliver information security content. The framework is developed based on insights from healthcare decision makers coupled with extensive literature study. The designed framework is implemented in the selected healthcare for further evaluation and to recognize which awareness training technique can best fit that particular organization.

TABLE I. POLICY AUGMENTATION

Policy	**UKM**	**ISO 27002 2005**	**SANS**	**HIPAA**
Software Application Security				
Control of Application Software	[√]	√	√	
Control of Unlicensed Software	[√]	[√]	[√]	
Control of Source Code Storage	[√]	[√]		
Control of Malicious and Defective Code Software	[√]	√		
Control of Malicious Code	[√]	[√]	[√]	√
Control of Version Changes	[√]	[√]		
Server Security				
Physical Security Control	[√]	√		
Control of Database	[√]	√		
Control of Logical Access	[√]	√		
User Identification	[√]	[√]	√	√
User Authentication	[√]	[√]	[√]	√
Information Back-up	[√]	[√]		
Maintenance	[√]	[√]		
Workstation Use			√	[√]
Network Tools Security				
Control of Network Tools Installation Security	[√]	√		
Control of Network Tool Configuration	[√]	√		
Control of Physical Security	[√]	√		
Control of Logical Access	[√]	√		
Wired Network	[√]	√		
Wireless Network (WIFI)	[√]	√		
Control of Network Equipment Maintenance	[√]	√		
Network Security				
User Accessibility	[√]	[√]		
Local Area Network	[√]	√		
Wireless Network (WIFI)	[√]	√		
Connection with other Networks	[√]	√	[√]	
Not Promoted Access	[√]	√		
Firewall	[√]	√		
Internet Policy			[√]	
E-mail Accounts Security				
Controls on the Use of E-mail Accounts	[√]	√	√	
Control of Mailbox Maintenance	[√]	√		
Controls on the Use of E-Mail Software	[√]	√		
Audit Trail	[√]	√	√	
ICT Security Incident Management	[√]	[√]		√

LEGEND:	
√	Available source
[√]	Selected source for augmentation

Literature [8] developed a framework to select an effective training delivery method. The framework is further improved and presented in Fig 4. The authors discussed that an effective awareness training program should be designed by giving significant thoughts to organizations' need as well as training success factors. The content of any training program must be tied to individual organization's need. Therefore, organizations should conduct a training need assessment survey prior to designing their awareness training program. Moreover, an effective information security awareness training program should be based on the training success factors defined by the organization.

A. *Organization Training Need Assessment*

Literature [22][6] stated that effective awareness training program cannot be developed without giving significant attentions to specific characteristics of an organization. Awareness raining programs should be tied to organizations' training need and requirements. Hence, it is important to conduct an organization training need assessment survey to obtain necessary information to develop training program. The results of the survey will provide justification to convince management for allocating adequate resources to meet the identified awareness and training needs. Literature [22][6] stated important training criteria to be investigated during the survey that include *organization size*, *business requirement*, *funding*, *target audience*, *organization mission and culture*, *organization rule and responsibility*.

B. *Training Development Plan*

The next step is to clarify the format of training program such as learning outcomes, length of training, target learners, overall format of training, overall description of the training, participant requirements, instructional material and aids needed, logistical issues. Training programs are developed with regards to the capability and requirement of an organization. For example, large organizations are likely to allocate more budgets on training program or they require more employees to participate in the program [11].

C. *Training Success Factors*

Literature [12][18] Foundation Report, 2010) introduced training success factors that are critical in effectiveness of a program. The success factors include *defining goal*, *motivation*, *fun*, *creativity*, *duration*, *enforce policies*, *organizational culture*, *audience profile*, *easy to understand*, *feedback and evaluation*, and *management support*. In order to obtain satisfactory training outcomes organizations should collect adequate information regarding the training success factors. An effective awareness training program promotes employees' willingness to participate in training activities. Satisfied employees are more encouraged to apply learned skills in their daily job activities.

Furthermore, this study brings together critical training successes factors suggested by previous surveys [12], Rudolph et al., 2002). The training success factors include learning process, time frame, population, training cost, coverage of topics, availability, fun, motivation, challenge, feedback and measurability, effectiveness, updatability, customization, and supervision. The illustrations of these critical factors are provided in Table 2. Although it may not be realistic to expect a training program to satisfy all the success factors, but decision makers should consider important elements related to their organization's need and the learning objectives.

Table 3 provides a side-by-side comparison of the commonly used techniques as suggested in [1]. This table is designed for easy utilization of the above technique selection for awareness training program framework. Some of the boxes in the table are marked by ¤ sign because some of the criteria are subjected to design and implantation approaches. For instance, there are two primary models of web-based instruction namely synchronous (instructor-facilitated) and asynchronous (self-directed, self-paced). Instruction can be delivered by a combination of static method (learning portals, hyperlinked pages, screen cam tutorials, streaming audio/video, and live Web broadcasts) that is categorized as passive learning process. Instruction can also be delivered by interactive method (threaded discussions, chats, and desk-top video conferencing) that is categorized as active learning process. Based on a guide to selection of awareness training program framework (Fig 4) and selection of awareness training program guidelines (Table 3), Organizations should be able to decide on the best awareness training program that best fit the organization.

VIII. Conclusion

Human errors are known as the most serious threats to information security in Electronic Health Record systems. Employees who interact with EHR systems need to be educated about the risks and hazards associated with information security. There is a wide range of information security awareness techniques. However, research is insufficient on effective information security awareness delivery methods. It is essential that effective awareness training delivery method is selected, designed, and implemented to ensure proper protection of the organizational assets. It could be of a great help for organizations to have a step-by-step guideline that provides them with the necessary information on how to select an effective training technique, which fulfills the organization's need and requirement. The authors developed a framework for effective transfer of training. The aim is empowering healthcare decision makers to easily select an effective awareness training program to deliver information security content. Nevertheless, other industries might benefit from the guidelines by applying minor modifications. In this paper training success factors are discussed as critical factors in selecting an effective delivery method. It also explains the process of augmentation of information security content based on internal policy and international standards that can be used as a guideline for healthcare organizations.

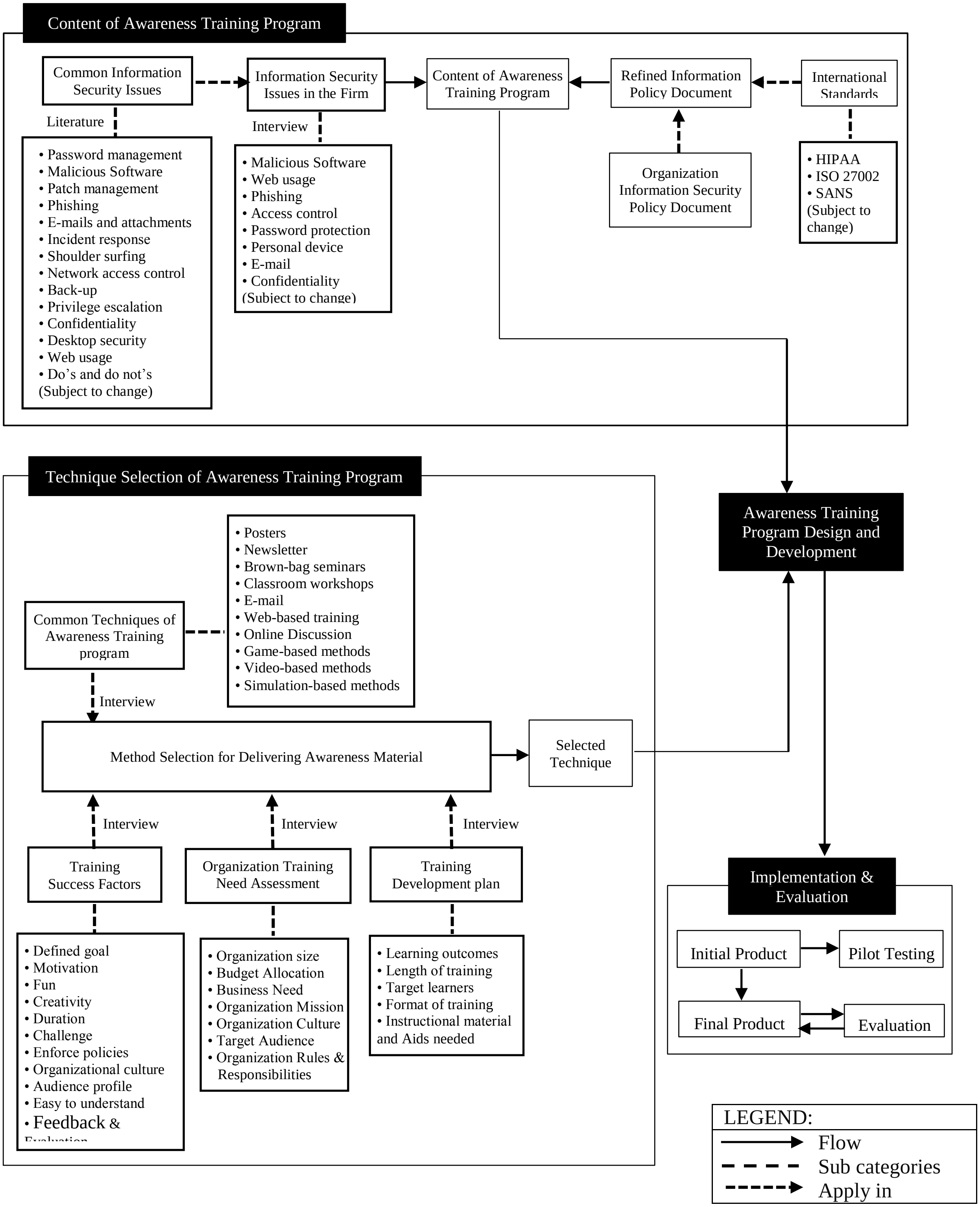

Fig. 4. A Guide to Selection of Awareness Training Program Framework

Source: Adapted from [8]

TABLE II. TRAINING SUCCESS FACTORS

Success Factor	Description
Learning Process	Training methods fit into two categories; active and passive. In Active learning the responsibility of learning lies with the learner. It covers all methods of training where the participants are involved and active in the learning process. In passive learning knowledge is directly transferred from one entity to another. It is normally a one way transfer from entity with more knowledge of the topic towards an entity with less knowledge.
Time Frame	Employee's daily job responsibilities require flexible schedule. each individual should be given sufficient time to participate in the training program and follow the process without worrying about affecting their performance at the workplace.
Population Coverage	Number of audience covered by an awareness training program.
Training Cost	Design and implementation cost of a training program.
Coverage of Topics	Some of the training techniques are suitable for disseminating of a single message, whereas others can be used for delivering a number of messages.
Content Updatability	Training content should be developed in a way that it allows trainers to update and modify the content if necessary.
Customization	Training contents should be tailor made to each organization based on their specific needs and requirements.
Fun	The amount of entertaining is directly related to individual learning. Participants should be given opportunities to have fun and enjoy what they are doing when engaged with training activities.
Motivation	Motivational factors are needed to encourage individuals to change the way they used to behave and operate.
Challenge	An effective training technique must challenge and engage the participants. Many programs fail to challenge the user which could lead to privation of self-motivation that may encumber successful delivery of the materials.
Supervision	In some training programs trainer directly lead and supervise the program. Whereas, some training programs are run without any supervision.
Feedback & Measurability	Every successful training program provides feedback to both trainees and instructors. Feedback and evaluation are the strengths of each training program and an easy way to distinguish effective trainings form non-effective ones. Trainers must measure and evaluate employees performance before and after training sessions.
Easily Accessible	It refers to the availability of training programs to the organizations and users. For instance, the availability of experienced trainers, training materials, location, and etc.

TABLE III. SELECTION OF AWARENESS TRAINING PROGRAM GUIDELINES

Training Delivery Method		**Awareness Training Program Development**												
		Success Factors									**Content**		**Implementation & Evaluation**	
		Active Learning Process	**Flexible Time Frame**	**Large Population Coverage**	**Low Cost**	**Multiple Topic Coverage**	**Easily Accessible**	**Fun**	**Motivation**	**Challenge**	**Content Updatability**	**Customization**	**Supervision**	**Feedback & Measurability**
Paper-based Methods	Posters	×	√	√	√	×	×	×	×	×	×	×	×	×
	Newsletter	×	√	√	√	×	¤	×	×	×	×	×	×	×
Instructor-led methods	Brown-bag seminars	×	×	×	√	×	×	×	¤	×	√	√	√	×
	Classroom workshops	×	×	×	¤	√	×	×	×	×	√	√	√	×
Online methods	E-mail	×	√	√	√	×	√	×	×	×	√	×	×	√
	Web-based training	¤	¤	¤	¤	√	√	¤	¤	¤	√	√	×	¤
	Online Discussion	√	×	×	√	√	√	√	√	√	√	√	√	¤
Game-based methods		√	√	√	×	√	√	√	√	¤	¤	¤	×	√
Video-based methods		×	√	√	×	√	√	×	×	×	×	×	×	×
Simulation-based methods		√	×	¤	×	×	×	√	√	√	¤	√	×	√

Source: [7], [1]

LEGEND:	
√	Applicable
×	Not applicable
¤	Subject to change

References

[1] J. Abawajy, “User preference of cyber security awareness delivery methods,” Behavior & Information Technology, Vol. 33, No. 3, pp 237–248, 2012.

[2] L. A. Annetta, “The “I’s” have it: a framework for serious educational game design,” Review of General Psychology, 14 (2), 105-112, 2010.

[3] T. Asai, and J. L. C. Perez, “Human-related problems in information security faced by Japanese, British and American overseas companies because of cultural differences,” China-USA Business Review, Vol. 11, No. 1, Pp 86-101, 2012.

[4] A. Bakhtyari Shahri, Z. Ismail, and N. Z. A. B Rahim, “Security effectiveness in health information system: through improving the human factors by education and training,” Australian Journal of Basic and Applied Sciences, 6, 226-233, 2012

[5] X. Y. Cheng, Y. M. Wang, and Z. L. Xu, “Risk assessment of human error in information security,” Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 2006.

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

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

[8] A. Ghazvini, Z. Shukur, “An effective awareness training program for information security in Hospital Universiti Kebangsaan Malaysia (HUKM),” Journal of Next Generation Information Technology. Vol. 6, No. 3, pp. 1-12, 2015.

[9] HIMSS Analytics. The 2010 HIMSS Analytics Report: Security of Patient Data. Technical Report. Available: http://www.mmc.com/views/Kroll_HIMSS_Study_April2010.pdf. 25 February 2014.

[10] E. F. Holton, “The flawed four-level evaluation model,” Human Resource Development Quarterly, vol. 7, no. 1, pp 5-21, 1996.

[11] I-TECH (International Training and Education Center for Health) (2012). Department of Global Health. University of Washington. Available: http://globalhealth.washington.edu/organization/international-training-education-center-health-i-tech

[12] S. Manke, and I. Winker, “The habits of highly effective security awareness program: a cross-computer comparison. internet security advisors group,” 2012.

[13] J. Mohan, and R. R. R. Yaacob, “The malaysian telehealth flagship application: a national approach to health data protection and utilization and consumer rights,” 2014.

[14] T. Monk, J. Niekerk, and R. Solms, “concealing the medicine: information security education through game play,” Institute for ICT Advancement, Nelson Mandela Metropolitan University, 2010.

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

[16] R. Parks, C. H. Chu, and H. Xu, “Healthcare information privacy research: issues, gaps and what next?,” 17th American Conference on Information Systems (AMCIS 2011), 4-8 August 2011 Detroit.

[17] Ponemon Institute. 2012. The human factor in data protection. Ponemon Institute. Available Online athttp://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf

[18] Rockefeller Foundation Report. (2010). From Silos to Systems: An overview of ehealth’s transformative power. Available: http://www.rockefellerfoundation.org/uploads/files/e331d255-059f-4fc6-b814-5938f8ee017e-rf.silos_1-13.pdf

[19] G. N. Samy, and R. Ahmad, “Threats to health information security,” The Fifth International Conference on Information Assurance and Security, 2009, Universiti Teknologi Malaysia (UTM), Malaysia.

[20] R. S. Shaw, C. C. Chen, L. A. Harris, H. J. Huang, “The impact of information richness on information security awareness training effectiveness,” Computers & Education, Vol. 52, No. 1, pp 92–100, 2009.

[21] N. Waly, R. Tassabehji, and M. Kamala, “Improving Organizational Information Security Management: The Impact of Training and Awareness,” IEEE 14th International Conference on High Performance Computing and Communications. Bradford University. United Kingdom, 2012.

[22] M. Wilson, J. Hash, “Building an information technology security awareness and training program,” National Institute of Standards and Technology (NIST), 2013. Available: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[23] S. Yamnill, G. N. McLean, “Theories supporting transfer of training,” Human Resource Development Quarterly, vol. 12, no. 2, pp 195-208, 2001.