International Journal of Security and Its Applications
Vol. 11, No. 7 (2017), pp.87-96
http://dx.doi.org/10.14257/ijsia.2017.11.7.07

Information Security Content Development for Awareness Training Programs in Healthcare

[*1]Arash Ghazvini and [2]Zarina Shukur

[12]*Faculty of Information Science and Technology,*
Universiti Kebangsaan Malaysia,
43600 UKM, Bangi Selangor, Malaysia
[1]*Email: arashgv@gmail.com*

Abstract

Human error is recognized as the major cause of data breaches across the healthcare industry. Training and education are effective approaches to help employees adhere to appropriate behaviors that do not compromise information assets. However, not all awareness training programs are effective. One of the main failures in implementing successful awareness programs is the training content. In many cases, the training content is reported to be too informative or too advance. The aim of this paper is to propose a guideline to develop information security content for awareness training programs. Developing a rich and attractive training content is the key to an effective awareness program. It is necessary to ensure that important information security issues are effectively communicated with employees during awareness training programs, and employees are not over-trained or under-trained. The paper demonstrates the process of information security policy augmentation for a selected healthcare organization, and develops information security content from the augmented policy document. The focus of the training content is to enforce the organization's internal information security policies.

Keywords: *Training Content, Information Security, Awareness Training Program, Electronic Health Record*

1. Introduction

The aim of this paper is to propose a guideline to develop information security content for information awareness training programs. Human error is recognized as the major cause of data security breaches across the healthcare industry [15,4,8]. The adaption of electronic health records (EHR) by healthcare organizations requires better safeguard information assets. EHR refers to document imaging or systems established in community health centers or medical practices that include patient health and identification information, medications and prescription records, and laboratory results [23].

Training and education are effective approaches to help employees adhere to appropriate behaviors that do not compromise information assets, and ultimately reduce information damages. Reference [23] reported that there has been a loss of health information in more than 110 healthcare organizations, which influenced over 5,306,000 individuals since January 2008, and the damage in 2010 has been amounted to $6 billion [21].

According to [14], a key to addressing security breaches is providing security awareness programs to increase employees' knowledge about security issues. Information security awareness refers to users' understanding of the importance of information security best practices [1]. The aim of information security awareness training programs is to enhance employees' perceptions, attitude, and motivation to learn and sustain appropriate behaviors toward information security [13]. Educating employees about

ISSN: 1738-9976 IJSIA

security and privacy issues can solve basic problems related to information security awareness.

However, not all awareness training programs are effective. The main failure to successfully implement awareness programs is the training content. In many cases, the training content is too informative or too advance [6]. If the training content is too professional or difficult to comprehend, employees may lose interest to participate in training activities. In the information security context, training materials are developed by experts who may not consider the targeted employees' profile. Hence, it is important to develop a training content that addresses both organizations and employees' needs. While enforcing organizations' internal information security policy document, the training content must be easily understood by the targeted audience.

Hence, this paper proposes a guideline that helps organizations to develop information security content for awareness training programs. Hospital Universiti Kebangsaan Malaysia (HUKM) is selected as the case healthcare organization to develop information security content. HUKM has implemented a number of awareness training programs that failed to produce a satisfactory outcome. This paper proposes information security policy augmentation for HUKM, and develops information security content from the augmented policy document. The focus of the training content is to enforce the organization's internal information security policies.

2. Information Security Training Content

Developing a training content for information security awareness programs highly depends on the organization [20] as different organizations deal with different information security issues [12]. Organizations need to identify specific issues to be addressed in awareness training programs. As stated by [12], the main items to cover during awareness training programs include:

- The organization's internal security policy
- The major threats to the organization's information assets
- Basic safeguards, e.g. choosing strong passwords
- Incident management

Reference [20] emphasized on organizations' internal information security policy as an important item to cover in the training content. Addressing the internal policy helps employees to understand the importance of information security and learn how to prevent incidents from happening.

The training content's aim is to help employees recognize information security issues and respond accordingly [5]. According to [6], a rich and attractive training content is the key to an effective awareness training program. The author stated that the training content should address employees' knowledge gap. Hence, training content should cover common information security mistakes made by employees [20]. Looking at employees' common mistakes helps to determine the level of security awareness training required for the organization, and to avoid over-train or under-train employees [20]. In a similar vein, [22] mentioned that the training content should be created based on the needs of the targeted audience.

It is important to ensure that employees understand the content being delivered [20] that leads to behavioral changes [12]. If the training content is not understood by employees, they may still unintentionally put information assets at risks. Hence, feedbacks about the training content and its comprehension are important to ensure employees understand the training content as well as the organization's internal information security policy [20].

Furthermore, reference [5] emphasized on the importance of content updatability. An awareness training program should enable instructors to modify training contents

according to assessment results and for post-training purposes. Content updatability refers to the flexibility of managing and customizing discussion and security topics and content.

Training is useless if it cannot be translated into performance [24]. Reference [16] emphasized the importance of training content in designing an effective training program. He argues that the training content is important to help learners to understand information and materials easily. Kemp's model emphasized on the importance of training content to enhance individual performance.

3. Training Content Development Guideline

Developing a rich and attractive training content is the key to an effective awareness training program [5]. It is necessary to ensure that important information security issues are effectively communicated with employees during awareness training programs, and employees are not over-trained or under-trained. Therefore, there is a need to develop a guideline for organizations to create information security content for awareness training programs. Figure 1 shows the training content development guideline for information security awareness training programs.

The training content should 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. An organization's internal information security policy is an important item to cover in the training content [25][12][20]. Addressing the internal policy helps employees to understand the importance of information security and learn how to prevent incidents from happening. Moreover, looking at employees' common mistakes helps decision makers to determine the level of security awareness training required for the organization to avoid over-train or under-train employees [20].

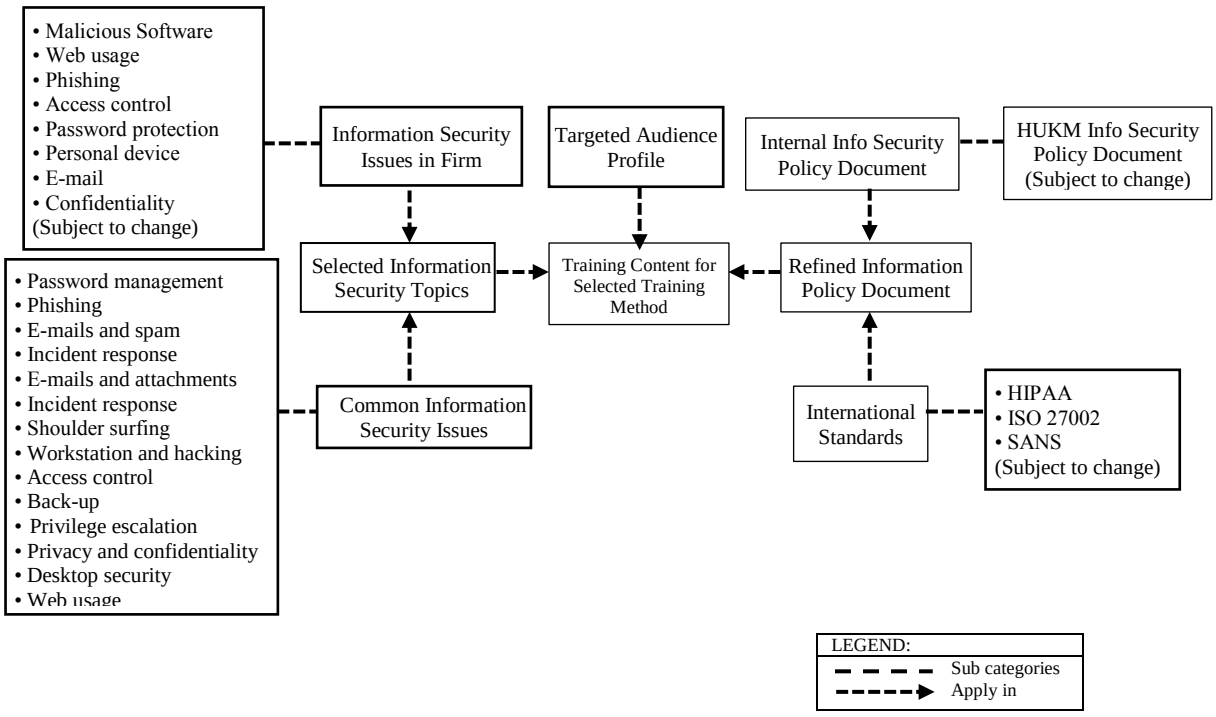

Figure 1. Training Content Development Guideline

3.1 Training Content for Selected Training Method

It is important to ensure that employees understand the delivered content, otherwise, they may involuntarily put corporate information at jeopardy. Therefore, obtaining feedback on the training content and employees' level of understanding is the key to confirm personnel comprehension of the content as well as corporate security policy. The structure of the training content depends on the selected training delivery method. For instance, awareness training programs that can facilitate feedback on the content can be in the format of multiple choice, true or false, short answer, fill in the blank, and essay to obtain feedback and test employees' understanding of the content.

3.2 Targeted Audience Profile

Information security content for selected awareness training programs should be based on the targeted audience profile. If the message is designed to be too hard to understand, it will drive beginners away, and if it is too easy, it will make professionals bored. For instance, general employees of a healthcare organization have basic knowledge of information security, therefore, the designed message should be easy to comprehend and not too informative.

3.3 Selected Information Security Topics

Organizations must identify common information security issues that frequently occur in the workplace by employees. Different organizations deal with different issues. Therefore, every organization must identify the issues to be addressed in the awareness training program. The identified issues must be used as references in the process of content development. Previous studies [2][18] identified the major threats to information security. These issues can be used as topics for awareness training programs. Table 1 presents the common information security topics awareness training programs. Organizations need to recognize which security information topics are applicable for the awareness training programs in their organization.

Table 1. Common Information Security Threats

Topic	Description
Password protection	To safeguard passwords, e.g. selecting strong passwords, changing passwords frequently
Malicious code	Protection from malicious codes, e.g. Trojan horses, worms, viruses
Patch management	Refers to security updates designed to fix problems with updating programs
Phishing	Attempt to obtain sensitive information, e.g. username and password
Emails and spam	To handle emails or attachments received from an unknown person or spam
Incident response	Managing security incidents, e.g. breach and attach
Shoulder surfing	Protection from spies who attempt to obtain personal access information
Workstation and hacking	Protection from hackers
Access control	Restriction access to private information assets
Back-up	Properly archiving information
Privilege escalation	Elevated access to private information
Privacy and confidentiality	Protection of private and confidential information

Topic	Description
Desktop security	Proper use of screensavers and prevent unauthorized individuals from obtaining information on screen
Web usage	Proper and safe web surfing

3.4 Information Security Issues in Firm

HUKM is selected as the case healthcare organization to develop a training content. The most common issues of information security systems in HUKM are determined through semi-structured interviews with key decision makers. Eight topics are recognized as the most common issues in HUKM, including: 1) phishing; 2) web using; 3) email and spam; 4) malicious code; 5) password protection; 6) privacy and confidentiality; 7) workstation and hacking; 8) access control.

3.5 Refined Information Security Policy Document

The content of information security awareness training programs must be driven from the organizations' internal information security policy. Organizations must ensure that their internal policy document is in line with international standards. Therefore, they should review and refine their existing information security policy based on the current trends. Although the policy should be tailor made and unique to each individual organization, they must follow the international information security standards [17].

3.6 International Standards

This paper refers to three international information security policy sources that can be used as the reference sources in the process of content creation for information security awareness training programs:

ISO 27002 provides information security standards and management practices while taking into account the information security environment of an organization. For instance, it provides the guideline on selecting, implementing, and managing information security standards [11].

The System Administration, Networking, and Security (SANS) institute provides information security policy and standards as a guideline for organizations to develop and implement security policies [19].

The Health Insurance Portability and Accountability Act (HIPAA) is introduced specifically to safeguard electronic health information. It aims to improve security standards and to protect confidential health information. It gives a guideline on how to record and store patients' health information before, during, and after electronic transmission [10].

4. Policy Augmentation

Table 2 demonstrates how HUKM's internal policy is augmented by taking "control of logical access" as an example. The left hand side column is a list of topics obtained from HUKM's policy document and international standards. The other four columns are policy sources including HUKM, ISO, SANS, and HIPAA. The first step is to gather a list of topics. The researcher reviewed HUKM's policy as well as the other three sources to identify what is missing in HUKM's documents. For instance, as shown by the table, HUKM does not have any policy regarding workstation use. The next step is to distinguish which topics are covered by each source, as indicated by the [√] in the table.

Subsequently, the strength and quality of the policy statement provided by each source are carefully evaluated in comparison with HUKM's policy statements. Policy statements

are extracted from the sources and incorporated into HUKM's policy document when necessary, as indicated by the [√].

Table 2. 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			√	[√]

4.1 Control of Logical Access

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

5. Training Content for HUKM

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

5.1 The Questions

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

5.2 The Wrong Answers

This study conducted a survey among healthcare employees to collect their own wrong answers in response to information security questions. The wrong answers are used to design the training content. This approach is helpful: i) to understand the knowledge level of employees about security topics; iii) to address employees' real problems 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 the form of open-ended structure and they are distributed among the employees. For example, many employees responded that the minimum length of strong password was four characters whereas the right answer was eight characters.

5.3 The Correct Answers

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

6. Conclusion

This paper proposes a guideline to develop information security content for awareness training programs. As suggested, the training content must be developed based on: i) the healthcare organization's 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 Hospital Universiti Kebangsaan Malaysia's (HUKM) internal policy document, in some parts, are not in line with the international standards. Therefore, this study proposes policy augmentation for HUKM. Subsequently, the training content is developed for HUKM based on the augmented policy document to enforce the internal information security policy document. It is hoped that this guideline could help many more organizations to ease the process of content creation.

Table 3. 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 5. 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 11. 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. 2. 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.

Table 4. 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 character)?** 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?** 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; C stands for correct

References

[1] J. Abawajy, "User Preference of Cyber Security Awareness Delivery Methods". Behavior & Information Technology, vol. 33, no. 3, **(2003)**, pp. 237–248.
[2] A. Ahmad, "Type of Security Threats and It's Prevention", International Journal of Computer Technology and Applications, vol. 3, no. 2, **(2012)**.
[3] M. Alhabeeb, A. Almuhaideb, P. D. Le and B. Srinivasan, "Information Security Threats Classification Pyramid", In Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference, **(2010)**.
[4] 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, **(2012)**, pp. 86-101.
[5] C. C. Chen, R. S. Shaw and S.C. Yang, "Mitigating information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System", Information Technology, Learning, and Performance Journal, vol. 24, no. 1, **(2006)**, pp. 1-14.
[6] B. D. Cone, C. E. Irvine, M. F. Thompson and T. D. Nguyen, "A Video Game for Cyber Security Training and Awareness", Computers & Security, vol. 26, **(2006)**, pp. 63-72.
[7] A. Ghazvini and 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, **(2015)**, pp. 1.
[8] HIMSS Analytics, "The 2008 HIMSS Analytics Report: Security of Patient Data", Technical Report.
[9] HIMSS Analytics, "The 2010 HIMSS Analytics Report: Security of Patient Data", Technical Report.
[10] HIPAA (The Health Insurance Portability and Accountability). 2014. www.hhs.gov/hipaa
[11] ISO (International Organization for Standrdization) 27002. Standards 2005. http://www.iso.org/iso/home/standards
[12] E. C. Johnson, "Security Awareness: Switch to a Better Programme", Network Security, vol. 2, **(2006)**, pp. 15-18.
[13] H. A. Kruger, L. Drevin, S. Flowerday and T. Steyn, "An Assessment of the Role of Cultural Factors in Information Security Awareness", In 2011 Information Security for South Africa, **(2011)**.
[14] R. Mahapatra and V. S. Lai, "Evaluating End-User Training Programs", Communications of the ACM, vol. 48, no. 1, **(2005)**, pp. 66-70.
[15] 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)**.

[16] G. R. Morrison, S. M. Ross, J. E. Kemp and H. Kalman, "Designing Effective Instruction", John Wiley & Sons, **(2004)**.
[17] Rockefeller Foundation Report, "From Silos to Systems: An Overview of eHealth's Transformative Power", **(2010)**.
[18] G. N. Samy, R. Ahmad, "Threats to health information security". The Fifth International Conference on Information Assurance and Security. Universiti Teknologi Malaysia (UTM), Malaysia **(2009)**.
[19] SANS (The System Administration, Networking, and Security). https://www.sans.org [22 May 2014].
[20] Security Standard Council. 2014. Information Supplement: Best Practices for Implementing a Security Awareness Program. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf
[21] D. J. Sedlack, G. P. S. Tejay, "Improving information security through technological frames of reference", Southern Association for Information Systems Conference, Atlanta, GA, USA. **(2011)**.
[22] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, "Analyzing Trajectories of Information Security Awareness", Information Technology & People, vol. 25, no. 3, **(2012)**, pp. 327-352.
[23] World Health Organization, "Electronic Health Records: Manual for Developing Countries", (2006). http://www.wpro.who.int/publications/docs/EHRmanual.pdf
[24] S. Yamnill and G. N. McLean, "Theories Supporting Transfer of Training", Human Resource Development Quarterly, vol. 12, no. 2, **(2001)**.
[25] R. Yanus and N. Shin, "Critical Success Factors for Mapping an Information Security Awareness Program", Proceedings of the Sixth Annual ISOneWorld Conference, Las Vegas, Nevada, **(2007)**.

