Information Security: Awareness and Training Program in the Middle East Universities

Mohammad S. Eyadat,
California State University, Dominguez Hills
Carso, California, USA
Email: meyadat [AT] csudh.edu

ABSTRACT---- ***An effective Security Awareness and Training (SAT) program enables organizational members to understand the organization's security strategies, know their responsibilities, and control risks that are caused by security incidents. Therefore, deploying a SAT program is one of the most important steps for any organization to assure that information assets are appropriately secured. The aim of this paper is into folds: first, to gain an insight and determine the information security awareness and training program levels in Middle Eastern higher education sector through a case study that examined 182 institute websites over eight countries. Second, to provide recommendations based on the findings that aid information security professionals to establish a new or improved existing awareness and training program. Literature showed that no study has been done on the SAT program at the level of the Middle Eastern region. However, there was a need to this investigation and therefore, it was a pioneering study at the region level in the field of information security.***

Keywords---- Information Security, Awareness Program, Training Program, IT Resources, Emerging Technology, Higher Education

1. INTRODUCTION

Emerging technology is the trend of higher education institutes to provide a better learning environment. This emergence has given institutes' community members different ways to access the most vital information including their information security. Exposing this type of data and information could affect an institute positively or non-positively according to the user educational level. Therefore, educating the user with the knowledge and skills that are needed to protect such important information become a must. The user should know the best methods to access and use these data and information as well as the vulnerabilities and threats that might associate with it because he/she will be the first to face such threats. Accordingly, the top management and the information security managers are trying to find the most effective technology tools to harden their accessing systems. Knowing that the management should have a balance in the use of technical and non-technical approaches to protect institutes resources (Kritzinger & Smith, 2008).

Information systems produce significant benefits to institutes when the users learn and use all of the system capabilities. However, one risk of data and information protection is the difficulty users may experience in understanding and executing the information security practices that are regulated by an institute security policies (Goel & Chengalur-Smith, 2010). So educating users and having a work force that is educated and more aware of security issues should play an important role in protecting institutes' information. Therefore, security environment should involve more than just investing in the security technologies. Integrating Security Awareness and Training (SAT) programs into the security technologies can provide reasonable assurance, so that employees will be equipped with the knowledge and skills to use the technology in place and to act responsibly and practicing safe computing habits (Kim, 2005). Hence, an effective SAT program can be a critical component in protecting an institute's information and systems. It explains the users' role in the area of information security and shows how they can play a vital part in the protection process. Thus, awareness and training should be provided to any user who has a contact with the institute's information and systems (Wu, Guynes, & John, 2012; Whitman, & Mattord, 2004).

The structure of this research paper is divided into eight sections. In the second section, awareness and training program background is presented. Third section presents the literature review. The need for SAT is presented in section four. Research methodology is explained in section five. Data analysis and results presented in section six. Conclusion and recommendations are presented in section seven then it is concluded by the limitation and future research section.

2. AWARENESS AND TRAINING PROGRAM BACKGROUND

2.1 Security Awareness Program

Security awareness is designed to modify any person behavior that endangers the security of the organization's information. It is the part of the training that puts the information into the short-term memory which should move that information into permanent application in the employee's everyday working environment (Gurman & Roback, 1995; Kim, 2014). Therefore, it installs a sense of responsibility, which leads users to care more on how to use their devices, what type of information to exchange, and what type of data and information to store in it. Moreover, it minimizes the risk of accidental compromise, damage, or destruction of information. Furthermore, security awareness program aim to generate behavioral outcomes that go beyond the procedural knowledge of using security defense mechanisms (Whitman & Mattord, 2012). This is because many security breaches result from human negligence and attackers focus on weaknesses in people or processes. Even one single employee's carelessness can undermine the best defense mechanism in place; thus, awareness programs also need to enhance the employee's capability for making sound security judgment and preventing negligence. (Wu, Guynes, & John, 2012).

Despite being an effective security method, the concept of security awareness is the least frequently implemented as noted in NIST Sp800-12 (Gurman & Roback, 1995). Many security awareness components are available at low costs, or virtually no cost except paying for the time and energy of the developer while others can be expensive (Androulidakis & Papapetros, 2008). A security awareness program can deliver its message in variety methods including videotapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, talks, lectures, or short reminder notice at logon. In addition, an organization can establish a webpage or a site dedicated to promoting information security awareness such as the capability of informing the employees via email when information related to security is posted.

Effective security awareness programs need to be designed with the recognition that tends to practice a tuning out process. For instance, a security poster will be ignored and blended into the environment regardless of how well it is designed. For this reason, awareness techniques should be creative and frequently updated (Gurman & Roback, 1995; Whitman & Mattord, 2014).

2.2 Security Training Program

Security training is defined in NIST Special Publication 800-16 as follows: "The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing)." Which is also cited in NIST Special Publication 800-50 by (Wilson & Hash, 2005). Accordingly, the security training program trains users to be equipped with the needed security skills in a manner controlling risks that may threaten organizations' resources and assets. Thus, user information security training program is quickly becoming an integral part of most organizations (Whitman & Mattord, 2012).

In regard to higher education world, there are several approaches that an institute can make its members active participants of a security training program. For example, regard to the students, an institute can implement effectively such as making virtual training a requirement of any computer courses, during a new student orientation session, and when students log on to a blackboard site at the beginning of each semester. By doing so, not only will students learn the necessary security concepts and skills but they will also update their security knowledge and be reminded of the importance of information security regularly (Kim, 2014).

Regarding to the faculty, staff, and administrators, the organization may utilize in house training, online training, or outside training. Online training is one of the staple crops of the information security training industry today. A properly designed online training course can be a cost effective solution to any organization's training requirements. Both in house and outsourced services can be utilized to create the training program, and either can be considered a cost effective solution. What really works well with online training is that content repositories can be set up according to the institute need. For example, if it is necessary to give the IT department personnel different training materials than the rest of the other employees, the training programs can certainly handle that. Conversely, if consistent training is required for all employees, online training programs can easily handle that as well. Additionally, online training programs can be very good at providing metrics and administrative support such as progress checking, grading quizzes, etc. Furthermore, online training is especially successful in large organizations where non-electronic training methods are invisible or too expensive. Online training however is not without its faults. Online training lacks the personality that any live training session inherently possesses. Also, the ability to stop and ask questions and interaction between the participants is simply not there. Many large organizations such as Workplace Answers and SANS have readily available training programs for any company. (SANS, 2015; Website: Workplace Answers, 2015). Regardless the deployed methodology, security training program is only effective if trainees are able to retain what they have learned and gathered. An organization can spend millions of dollars securing their networks, hiring consultants, and hardening their systems. However, without proper security training of the authorized users, these efforts will be futile.

3. LITERATURE REVIEW

Emerging technologies are becoming an essential element of a higher education environment. For example a mobile device is an efficient communication device and a vital part of daily life for billions of people around the world. Regardless the purpose of their use, educational, personal, or business, the mobile devices have contributed to the escalated growth of m-education (Traxler, 2007).

In m-education environment, students use information technology and information systems extensively for many reasons such as: taking online courses, using the blackboard system, using e-mail, accessing social networks, and using their smart phones, iPads, and PCs. Therefore, it is very important that they have the minimum knowledge and skills to protect their information and systems from possible security attacks (Kim, 2014; Androulidakis & Kandus, 2011; Traxler, 2007). According to Kim, Mims, and Holmes (2006), to deploy the emerging technologies successfully required the awareness of the security issues might encounter while using these technologies. Therefore, a proper awareness and training programs should be available for the administrators, educators, and students because having uneducated users, an institute is taking a very large risk in putting the security of the entire institute into the hands of a very few security professionals that cannot fully secure the information with only the help of technology. This risk can be extremely minimized through the implementation of a successful SAT (Marks & Rezgu, 2009; Shaw, Chen, Harris, & Huang, 2009).

A case study for examining m-learning by exploring the pedagogical application of WhatsApp mobile software is conducted by Bere (2013), who reported that mobile security threats negatively affected the usage of WhatsApp application for learning. The report presented the concern of security as one of the most challenging issues.

Androulidakis and Kandus (2011) revealed in their study that users were unaware of the necessary measures to avoid a possible unauthorized access and/or sensitive data retrieval from their devices, which indicated the lack of knowledge in securing the protection of their data and information. Therefore, there is a need for promoting information security standards and practices within an organization and proposes that all users should be aware of disciplinary actions resulting from non-compliance with the organization's information security procedures (Katz, 2005; Eyadat and Al Sharyoufi, 2014).

Veiga and Martins, (2015) indicated that change management, information security program, and training and awareness dimensions would influence the information security management dimension positively. It is important to note that all three dimensions include aspects of training. This reinforces the value of training as a good avenue to improve information security.

It has been reported that the lack of awareness and non-compliance poses serious risks for the organization and should be properly assessed and mitigated as part of the organization's overall risk assessment strategies (Chan & Mubarak, 2012; Yeo, Rahim & Miri, 2007). Fatani, Zamzami, Aydin, and Aliyu, (2013) approved that security issues affected the privacy of student's data and also they indicated that student's awareness level was low.

4. THE NEED FOR AWARENESS AND TRAINING PROGRAMS

The continuous adoption of emerging technologies by the government, public, and private sectors to conduct business has influenced many other sectors, including educational institutes to move their operations online. The increase of such movement leads to increase number of victims to different types of attacks and the number of cybercrimes (Eyadat, 2015). Furthermore, security breaches and the compromise of sensitive data are serious growing concerns for students, faculty, and staff; thus, information security is become a major concern of an organizational management.

Security technology systems including intrusion prevention and detection systems, firewalls, anti-malware applications are key points for securing an institutes' data and information. However, with the deploy of emerging technology and the available advance tools to hackers and thieves, an effective information security awareness and training program can be a critical component to fortify an institute's information and systems security. Kraemer & Carayon (2007) also indicated that Information security training is a significant component of an institute's defense against information security attacks and breaches. Kim (2005) reported "If an organization is not able to effectively train its employees on information security standards and procedures, it may lead to less secure computing practices/behavior which could result in increased information security attacks and data breaches." For example, an institute's member may do not know the importance of backing up files unless they learn it from their security training (Kim, 2014).

It has been reported that awareness and training programs is an essential component to foster a strong information security culture across an organization (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012; Kritzingera & Smithb, 2008; Wu, Guynes, & John, 2012; Veiga, & Martins, 2015; Chan & Mubarak, 2012; Krugera, & Kearneyb, 2006).

According to Spears and Barki (2010) users' participation in security risk management contributes to greater organizational awareness of information systems security. Therefore, it is recommended that the organization should

include information security awareness as part of its overall risk assessment strategies in order to mitigate such risks (Chan & Mubarak, 2012; Yeo, Rahim, & Miri, 2007; Veiga, & Martins, 2015).

Despite of the availability of the information security technology and official organization standards, many researchers reported that there is still a high percentage of higher education institutes do not have adequate security awareness and /or training programs in place (Chan & Mubarak, 2012; Eyadat & Al Sharyoufi, 2014; Kim, 2014). Furthermore, a good number of higher education institutes offer no SAT program to their professionals and users, for example Marks and Rezgui (2009) reported that only third of the surveyed 435 higher education institutions had a training and /or awareness programs. Also Androulidakis and Kandus (2011) indicated that a high percentage of higher education institutes reported that they have no formal training and /or awareness programs for their community members.

In addition, nowadays, it is become mandatory to integrate and implement Security Education, Training, and Awareness program into organizational management systems, particularly in certain sectors. For example in health care industry, HIPAA (Hjort, 2003) section 164.308(a) states that covered entities must "implement a security awareness and training program for all members of its workforce (including management)." In the Defense Security Service's (DSS), the DSS Academy offers education and training programs in the security arena to the Department of Defense (DoD) and other U.S. government's personnel, employees, and contractors (DSS, 2018).

5. METHODOLOGY

One-hundred eighty-two websites of higher education institutes from eight countries (Saudi Arabia, United Emirate, Iraq, Jordan, Syria, Bahrain, Kuwait, and Qatar) in the Middle Eastern region were examined to understand the types and the extent of the SAT program included on the institutes' websites. Using two different browsers, Internet Explorer and Google Chrome, each site of the institute was surfed three to five times during the research period in 2013. Updates on the SAT of the examined institute sites were recorded through the repetitive visitations.

6. DATA ANALYSES AND RESULTS

Quantitative data analysis was conducted on the data collected from 182 Middle Eastern institute websites.

Frequency and relative frequency of the adoption of the individual category of the SAT program, namely, security awareness program, and security training program examined from the 182 institutes' websites were displayed in Tables 1 & 2, respectively. Out of the total of 182 institutes examined, 52 (29%) institutes deployed the security awareness program and 33 (18%) institutes deployed the training program. These alarming low adoption rates indicate that more than two-thirds (71%) and more than three-fourths (82%) of the examined institutes having no awareness program and training program, respectively, set in place. Therefore, authors recommended that a tremendous effort of convincing the senior top management of setting up the SAT program should be seriously considered by the information security professionals and managers to protect the resources and assets of their institutes.

Table 1. Frequency (Relative Frequency) of Awareness Program Adoption by Country

Country	No. of Institutes	Awareness Program	
		Adoption	No Adoption
Saudi Arabia	59 (100%)	26 (46%)	33 (54%)
United Emirate	35 (100%)	11 (31%)	24 (69%)
Iraq	30 (100%)	3 (10%)	27 (90%)
Jordan	26 (100%)	6 (12%)	20 (88%)
Syria	13 (100%)	1 (8%)	12 (92%)
Bahrain	11 (100%)	3 (27%)	8 (73%)
Kuwait	5 (100%)	1 (20%)	4 (80%)
Qatar	3 (100%)	1 (33%)	2 (67%)
Total	182 (100%)	52 (29%)	130 (71%)

Table 2. Frequency (Relative Frequency) of Training Program Adoption by Country

Country	No. of Institutes	Training Program	
		Adoption	No Adoption
Saudi Arabia	59 (100%)	18 (31%)	41 (69%)
United Emirate	35 (100%)	8 (23%)	27 (77%)
Iraq	30 (100%)	3 (10%)	27 (90%)
Jordan	26 (100%)	2 (8%)	24 (92%)
Syria	13 (100%)	0 (0%)	13 (100%)
Bahrain	11 (100%)	2 (18%)	9 (82%)
Kuwait	5 (100%)	0 (0%)	5 (100%)
Qatar	3 (100%)	0 (0%)	3 (100%)
Total	182 (100%)	33 (18%)	149 (82%)

Among the examined eight countries, Saudi Arabia recorded the highest rate of 46% in adoption of the awareness program within its own country while Syria recorded the lowest rate of 8%. Although not a single one country examined had an adoption rate of the awareness program exceeding 50% of the total number of institutes within its own country, the ratio of adoption vs. non-adoption of the awareness program was nearly one to one among the examined institutes in Saudi Arabia (Table 1). The trend of training program adoption was low among the countries examined. In particular, Qatar, Kuwait, and Syria had none of their institutes deployed a training program. Less than one-third of the institutes in each of the remaining five countries deployed the training program. Saudi Arabia appeared to be the lead with an adoption rate of 31% (Table 2).

Considering the adoption of the SAT program (including both of the awareness and training programs), the results revealed that among the 182 institutes examined, only 29 (16%) of them deployed both awareness and training programs (Table 3). That is, fewer than one in five institutes (16%) adopted proper safety measurement with a full adoption of SAT program. From the examined institutes' websites, 127 (70%) were recorded as having neither complete nor partial SAT program adoption. This translates into a tremendous high rate of the institutes examined were at high risk and vulnerable to the information security attacks. Among the three countries, Syria, Kuwait, and Qatar, where none of their institutes deployed full adoption of SAT program, the percentage of none adoption in Syria reached to 92%. That is, 12 out of 13 examined institutes in Syria were completely lack of awareness and training programs. Among the five countries, Saudi Arabia had the highest full adoption rate of 29%, followed by United Emirate (20%), Bahrain (18%), Iraq (7%), and Jordan (4%).

Table 3. Frequency (Relative Frequency) of SAT Program Adoption by Country

Country	No. of Institutes	SAT Program		
		Full Adoption	Partial Adoption	No Adoption
Saudi Arabia	59 (100%)	17 (29%)	9 (15%)	33 (56%)
United Emirate	35 (100%)	7 (20%)	5 (14%)	23 (66%)
Iraq	30 (100%)	2 (7%)	2 (7%)	26 (86%)
Jordan	26 (100%)	1 (4%)	6 (23%)	19 (73%)
Syria	13 (100%)	0 (0%)	1 (8%)	12 (92%)
Bahrain	11 (100%)	2 (18%)	1 (10%)	8 (72%)
Kuwait	5 (100%)	0 (0%)	1 (20%)	4 (80%)
Qatar	3 (100%)	0 (0%)	1 (33%)	2 (67%)
Total	182 (100%)	29 (16%)	26 (14%)	127 (70%)

The results reflect the deficiencies in regard to the security awareness and training program. The importance of implementation of the SAT program is urgent for suppressing the potential vulnerability to the internal and external threats. This imposes institutes' strategies to the emphasis of the importance of developing a SAT program.

7. CONCLUSION AND RECOMMENDATIONS

Due to the rapid evolution of the new technologies, the end users should receive proper training to avoid the potential threats that may cause the damage or loss of personal data. The management of higher education institutes should provide its community members the opportunity to acquire the essential information security knowledge through the SAT program since it is considered an essential part of defending information system security and offers the chance of communicating with the users in regard to the organization's information system security policies. The increase of the knowledge on security issues prepares the better practice of institute's community members, which in turn protects the system resources. Therefore, an information system without SAT program is vulnerable and prone to be hacked.

This research investigated the state of the SAT program employed by the higher education sector in the Middle Eastern region, in order to identify the extent of the SAT program. The study discovered an alarming and troublesome

low rate of having security awareness and training programs in place. The results indicate that a high percentage (70%) of the examined institutes offer no SAT program and only 30% of the examined institutes offer a complete or partial SAT program. The results are aligned to the literature survey findings. A review of the literature in the field of information security programs within higher education communities shows a high percentage in the lacking of the adequate knowledge and practice of SAT program due to the unavailability of such program in most of the higher education institutes (Marks & Rezgui, 2009; Androulidakis & Kandus, 2011).

The research also indicated that investment in all areas (technical and non-technical) of security is needed to effectively protect data and information assets. It provides management with a better understanding of the implications of security decisions under a variety of different conditions; furthermore, it assists professionals and managers in making better decisions concerning information security (Nazareth & Choi, 2015).

It shows that the unawareness of the SAT program leads to an increase in potential threats that could leave institutes' resources and assets at risk in particular with the increasing popularity of online learning. It is, therefore, recommended that a higher education institute should offer a formal information SAT program, a key factor to the successful use of IT resources, to secure their educational environment. In addition, the SAT program should include a clear ethical policy to faculty, staff, and students. It should incorporate clear definitions of user responsibilities for information security and ensure that strong restrictions are in place. Furthermore, an institution must conduct follow up SAT activities on a regular basis to ensure that the users comprehend and trust their IT security policy. Follow-ups should also be performed for staff members who configure and use security technologies. It is important for an institute's administrator to acknowledge that in order for security awareness and training programs to make a significant contribution to the field of information security, it is necessary to have a structured approach for measuring the effect of the SAT program prior to its implementation. (Kruger & Kearney, 2006)

8. RESEARCH LIMITATIONS AND FUTURE RESEARCH

The study was limited to the data collected from institute websites. An online survey soliciting the opinions of managers and professionals at different management levels from the examined institutes is recommended. The opinions could be qualitatively analyzed to develop a framework that aid the examined institutions in designing and developing an effective SAT program that cooperates the region's religious and cultural background.

9. REFERENCES

- Androulidakis, I. & Kandus, G. What university students do (or don't) know about security in their mobile phones. Telfor Journal, vol. 3, no. 1, 2011.
- Androulidakis, I., & Papapetros, D. Survey findings towards awareness of mobile phones' security issues. Proceedings of the 7th WSEAS International Conference on Data Networks, Communications, and Computers, 2008.
- Bere, A. Using mobile instant messaging to leverage learner participation and transform pedagogy at a South African University of Technology. British Journal of Educational Technology. Vol. 44, no.4, pp. 544–561, 2013.
- Chan, H. & Mubarak, S. Significance of Information Security Awareness in the Higher Education Sector. *International* Journal of Computer Applications, vol. 60, no. 10, pp. 887 – 975, 2012.
- Defense Security Service (DSS). Retrieved February, 201, from http://www.cdse.edu/index.html, 2018.
- Eyadat, M. Information security SETA program status at Jordanian Universities. Journal of Information Privacy and Security, Volume 11, no 3, pp 174 – 181. 2015.
- Eyadat, M., & Al Sharyoufi, R. Students awareness toward mobile wireless technologies security issues at college of computer science & computer engineering-Taibah University. The Journal of International Management Studies, vol. 14, no. 3, pp. 35-46, 2014.
- Fatani, H.A., Zamzami, I.F., Aydin, M., & Aliyu, M. Awareness toward wireless security policy: Case study of International Islamic University Malaysia. In the Proceeding of Information and Communication Technology for the Muslim World (ICT4M), 5th International Conference, pp.1 – 5, 2013.
- Goel S. & Chengalur-Smith I. Metrics for characterizing the form of security policies. Journal Strategic Inf Syst, vol. 19, no. 4, pp281-295, 2010.
- Gurman, B. & Roback, E. National institute of standards and technology, an introduction to computer Security: The NIST SP800-12, 1995.
- Montesdioca, G. P. Z., and Maçada, A. C. G. Measuring user satisfaction with information security practices. Journal Computers and Security. Vol. 48, Issue, pp 267-280, 2015.
- Hjort, B. HIPAA Privacy and Security Training. AHiMA Body of Knowledge website, Retrieved April, 13, 2017 from *http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_022114.hcsp*
- Katz, F. The effect of a university information security survey on instructing methods in information security. Proceeding on Information Security Curriculum Development, pp.43-48, 2005.

- Kim, E. B. Information security awareness status of full time employees. The Business Review, Cambridge, vol. 3, no.2, pp. 219-226, 2005.
- Kim, E. B. Recommendations for information security awareness training for college students. Information Management & Computer Security. Vol. 22, no.1, pp. 115-126, 2014.
- Kim, S.H., Mims, C., & Holmes, K.P. An introduction to current trends and benefits of mobile wireless technology use in higher education. AACE Journal, vol. 14, no. 1, pp. 77-100, 2006.
- Kritzinger, E. & Smith, E. Information security management: An information security retrieval and awareness model for industry. Computers & security, vol. 27, pp. 224–231, 2008.
- Kruger, H.A., Kearney W. D. A prototype for assessing information security awareness. Computers & Security, Vol. 25, Issue 4, pp 289-296, 2006.
- Marks, A., & Rezgu, Y. A comparative study of information security awareness in higher education based on the concept of design theorizing. In the proceeding of IEEE, pp 1-7, 2009.
- Nazareth, D. L., & Choi J. "A system dynamics model for information security management", Journal of Information & Management, Vol. 52 Issue 1, pp 123-134, 2015.
- SANS, Online security training. Retrieved May, 10, 2017, from http://www.sans.org/online-security-training/
- Shaw, R., Chen, C., Harris, A., & Huang, H., The impact of information richness on information security awareness training effectiveness. Computers & Educations, vol. 22, no. 1, PP. 92–100, 2009.
- Spears, J. & Barki, H., User participation in information systems security risk management, MIS Quarterly, vol. 34, no. 3, pp. 503-22, 2010.
- Traxler, J., Defining, discussing and evaluating mobile learning: The moving finger writes and having writ. International Review on Research in Open and Distance Learning, 8(2). Retrieved September, 30, 2017, from http://www.irrodl.org/index.php/irrodl/article/view/346/875
- Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E., Analyzing trajectories of information security awareness. Information Technology & People, vol. 25 No. 3, pp. 327-352, 2012.
- Veiga, A, & Martins N., Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, vol. 49, pp. 162-176, 2015
- Whitman, M. E. & Mattord, H. J., Making users mindful of IT security; awareness training is vital to keeping the idea of IT security uppermost in employees' minds. Security Management, vol.48, no. 11, pp. 32-34, 2004,
- Whitman, M. E. & Mattord, H. J., Principles of information security (4th Ed.). Course Technology, Boston, USA, 2012.
- Whitman, M. E., & Mattord, H.J., Management of information security (4th Ed.). Course Technology, Boston, USA, 2014.
- Wilson, M. & Hash, J., National institute of standards and technology, building an information technology security awareness and training program: The NIST SP800-50, 2005.
- Workplace Answers, Prevent Cyber Vulnerability: Online Training in Data Privacy and Security. Retrieved May, 10, 2018, from http://www.campusanswers.com/data-privacy-and-security/
- Wu, Y., Guynes, C., & John, W., Security awareness programs. Review of Business Information Systems – Fourth Quarter, vol. 16, no. 4, 2012
- Yeo, A., Rahim, M. & Miri L., Understanding factors affecting success of information security risk assessment: the case of an Australian higher educational institution. In the Proceedings of the Pacific Asia Conference on Information Systems, Auckland, 2007.