Higher Education Administrators Roles in Fortification of Information Security Program

Mohammad S. Eyadat
Associate Professor
CIS Department
California State University Dominguez Hills
Carson, California, USA, 90747

ABSTRACT

Information systems produce significant benefits to organizations. Therefore, organizations invest tremendous amount of money and time to obtain and manage information in order to maintain a high level of performance and to remain competitive. There are many factors that can impact the organizational information management and performance. One of the significant factors is to keep organizational environment secure. Information Security program is considered as one of the key factors for making organizational environment more secure and efficient. The aim of this research is twofold: first, to investigate the impact of higher education administrators' roles in strengthen the institutional information security system. Second, to explore the state and the importance of information security program in higher education. This research paper is based on theoretical of the existing information security strategic and approaches and a case study conducted at 59 institutes. The findings indicated the lack support and supervision of the top management for information security program. An alarming and troublesome high rate of unawareness of security with no education and training programs available in the surveyed institutes. The lack of adequate knowledge and security implementation among the majority of the communities of the surveyed institutes showed the need to activate the roles of the administrators to deploy a well-designed information security system.

INTRODUCTION

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. This caused the higher education to move and expand their teaching modality and services and the trend toward online services. The new trend imposes institutes' administrations to allow their community members (faculty, students and staff) utilizing their mobile devices in addition to standard computer devices to do their work. Additionally, it provides relatively open access to its community members and the public off-campus communities (parents, alumni, and cooperating industries).

The increase of such movement leads to increase number of victims to different types of attacks and the number of cybercrimes. There are variety of reasons for the increase of information security incidences including but not limited to electronic data, mobile devices, and lack of information technology (IT) security knowledge among Internet users. "The users are the weakest link which hackers use to break into an organization" (Katz, 2005). Unintentional mistakes caused by the users such as downloading unknown-source attachments are considered one of the top threats to information security in an organization (Whitman & Mattord, 2012). Therefore, a program such as Information Security Education, Training, and Awareness program that continuously educating professionals and users how to utilize the new and advanced security technology is indeed in dire need. Hereafter, the acronym "*InfoSec*" in this paper will refer to any Information Security program including Education, Training, and Awareness programs.

Despite the availability of the information security technology and official organization standards, a high percentage of higher education institutes offer no *InfoSec* to their professionals and users. Refereeing to Marks and Rezgui (2009), only third of the surveyed 435 higher education institutions had a complete or partial *InfoSec* program. Androulidakis and Kandus (2011) stated that 66% of higher education institutes reported that they have no formal *InfoSec* program for their community members.

InfoSec program plays a significant role in the process of the overall information security system and should be offered by higher education institutions. Pressure toward having this program in place is likely to come from faculty and the student body, which increasingly handling mobile devices and using them as support tools to their course work-study. Therefore, initiating and implementing an *InfoSec* program in higher education environment becomes a must and crucial.

The remaining of this paper is constructed in 8 sections. Section two discusses *InfoSec* program background. Section three, presents the literature review of the *InfoSec* program. Section four describes the methodology employed in this research. Section five discusses the data analysis and research findings. Section six highlights the importance of the administrators' roles. Conclusion and recommendations are elaborated in section seven. Finally, limitations of the study and future research are discussed and proposed in section eight.

INFORMATION SECURITY PROGRAM BACKGROUND

InfoSec program enhances educational and training programs by focusing on information security. The purpose of *InfoSec* is to enhance security in three ways: first, building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. Second, developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely. Third, improving awareness of the need to protect system resources (Whitman & Mattord, 2012). The following subsections present a brief description to the three components of the *InfoSec* program.

Security education

Security Education is defined in National Institute of Standards and Technology (NIST) Special Publication 800-16 as follows: "The 'Education' level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response." (as cited in Wilson & Hash, 2005, p. 9)

Security Training

The component of security training in the *InfoSec* program trains employees to be equipped with the needed security skills in a manner controlling risks that may threaten organizations' resources and assets. End-user security training component is quickly becoming an integral part of every organization, in particular the large ones (Vacca, 2009; Herold, 2010). An organization may 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.

Several methodologies including traditional face-to-face, computer based, online, and a combination of both (face-face, and computer based) can be used to conduct a security training program. Regardless the deployed methodology, security training program is only effective if trainees are able to retain what they have learned and gathered (Herold, 2010).

Security Awareness

Security awareness is designed to modify any person behavior that endangers the security of the organization's information. It keeps information security at the forefront of users' minds on a daily basis (Kritzinger & Smith, 2008). 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. 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 via videotapes, newsletters, posters, bulletin boards, flyers, demonstrations, briefings, talks, lectures, or short reminder notice at logon. 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).

INFORMATION SECURITY PROGRAM EFFECTIVENESS

InfoSec is like any other program that is intended to be implemented in a company, it must be measurable, if the program has not measurable outcomes then management will not be able to determine the effectiveness and savings obtained and may not be willing to invest in such programs. Fortunately, there are several models that are available to measure *InfoSec* program effectiveness. Human Performance Technology (HPT) also referred to as the science of improving human performance is one of the measureable models. HPT is the field of work that uses an engineering approach to attain desired results from human beings. Based in various tenets, the model has a systematic approach comprises several components including: Performance Analysis and Evaluation (Formative, Summative, and Confirmative). Explanation to HPT model is detailed in (Frank S. Wilmoth, Christine Prigmore, and Marty Bray, 2002), (what is HPT, 2014).

Return on Security Investment (ROSI) analysis is another tool that allows for the justification of investments and projects before senior management and the finance department making implementation decision. Also it could help top management administrators to determine the economic savings incurred with the implementation of the *InfoSec* program. (Lockstep Consulting, 2004)

LITERATURE REVIEW

Emerging technologies including mobile devices are becoming an essential element of a higher education environment. 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, for entertainment or business, the mobile devices have contributed to the escalated growth of the m-education (Traxler, 2007).

The use of mobile technologies can overcome the limitation of educational flexibility with wired technology. The advantages of mobility and mobile wireless technologies help improve efficiency and effectiveness of teaching and learning process (Ally, 2009), but at the same time it raised many challenges particularly the security issues which would be suppressed by deploying the *InfoSec* program.

Thomson and Solms (1998) reported that *InfoSec* program plays a significant role in the process of strengthening the overall information security in organizations, especially in the context of higher education environments. According to Katz (2005) and Eyadat (2015) there is a need for promoting information security standards and practices within an organization and they proposed that all users should be aware of disciplinary actions resulting from non-compliance with the organization's information security procedures. A successful organizational information security policy should incorporate clear definitions of user responsibilities for information security (Gaunt, 2000; Whitman & Mattord, 2014). Similarly, Banerjee, Cronan, and Jones (1998) reported that organizations should introduce information security awareness and make their ethical policy clear to their employees and ensure that strong deterrents are in place. As an information security professional, the researcher strongly believes these could be achieved through implementing *InfoSec* program in an organization's information systems.

Kim, Mims, and Holmes (2006) indicated that college students possess basic knowledge of most information security topics recommended by NIST Special Report 800-50. In the same report, they recommended that institutes should provide easily accessible security training programs for their students in order to have an effective *InfoSec* program.

Another recent case study conducted by Bere (2013) examining m-learning by exploring the pedagogical application of WhatsApp mobile software. Bere suggested that mobile security threats negatively affected the usage of WhatsApp application for learning. The suggestion was based on several factors. The concern of security was one of the most challenging factors. Fatani, Zamzami, Aydin, and Aliyu, (2013) approved that security issues affected the privacy of student's data. They also indicated that student's awareness level was low. Moreover, Androulidakis and Kandus (2011) and Eyadat and Al Sharyoufi (2014) revealed in their studies 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.

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 *InfoSec* program should be available for institutes' on-campus and off-campus users

METHODOLOGY

Fifty-nine websites of higher education institutes in Saudi Arabia were examined to understand the types and the extent of the *InfoSec* program included on the institute 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 *InfoSec* program of the examined institute sites were recorded through the repetitive visitations.

Information security professionals and managers from one of the examined institutes were contacted and invited for face-to-face interview following the preliminary website results. Based on their availability, a group of 8 professionals was non-randomly selected and interviewed for their insights on the involvement of the administrators and on the level of *InfoSec* program implemented. Interview questions were adopted and modified from NIST 800-50 (Wilson & Hash, 2005) to reflect the initial findings from the preliminary website results.

DATA ANALYSES AND RESULTS

Quantitative data analysis was conducted on the data collected from 59 Saudi Arabian Institute websites as well as the interview data collected from the information security professional staff worked in one of the surveyed institutes.

WEBSITE DATA ANALYSIS

From the examined 59 Saudi Arabian Institute websites, 32 were recorded as having neither complete nor partial information security program in place as shown in table 1 and figure1. This translates into more than half (54%) of the institutes examined were at high risk and vulnerable to the information security attacks. Tremendous efforts of convincing the top management administrators to put *InfoSec* program in place should be seriously considered by the information security professionals and managers to protect the resources and assets of the institutes.

Table 1
Security Program Adoption
In 59 Saudi Arabian Institutes

InfoSec Program–Components Deployed	Number of Institutes	%
1, 2, or 3 Components	27	46%
none of the three Components	32	54%

Frequency and relative frequency of the adoption of the individual category of the *InfoSec* program, namely, security education, security training, and security awareness, from the 59 institute websites examined were displayed in Table 2 and Figure 2.

Twenty-Seven institutes deployed one or more of three components (Table1, Figure1). Of the Twenty-Seven institutes having *InfoSec* program in place, 26 of them have either a complete or a partial awareness component implemented. (Tables 2). Seventeen of them only had the three components implemented, namely, security education, training, and awareness (table3). The remaining 10 institutes, one of them implemented only one component, namely, training security program. The other 9 institutes implemented only the awareness security program (Table 4). The results reflect deficient attention in regard to the security awareness, training, and education. The importance of implementation of the *InfoSec* program is urgent for suppressing the potential vulnerability to the internal and external threats.

Figure 1
Program Deployed in 59 Saudi Arabian Institutes

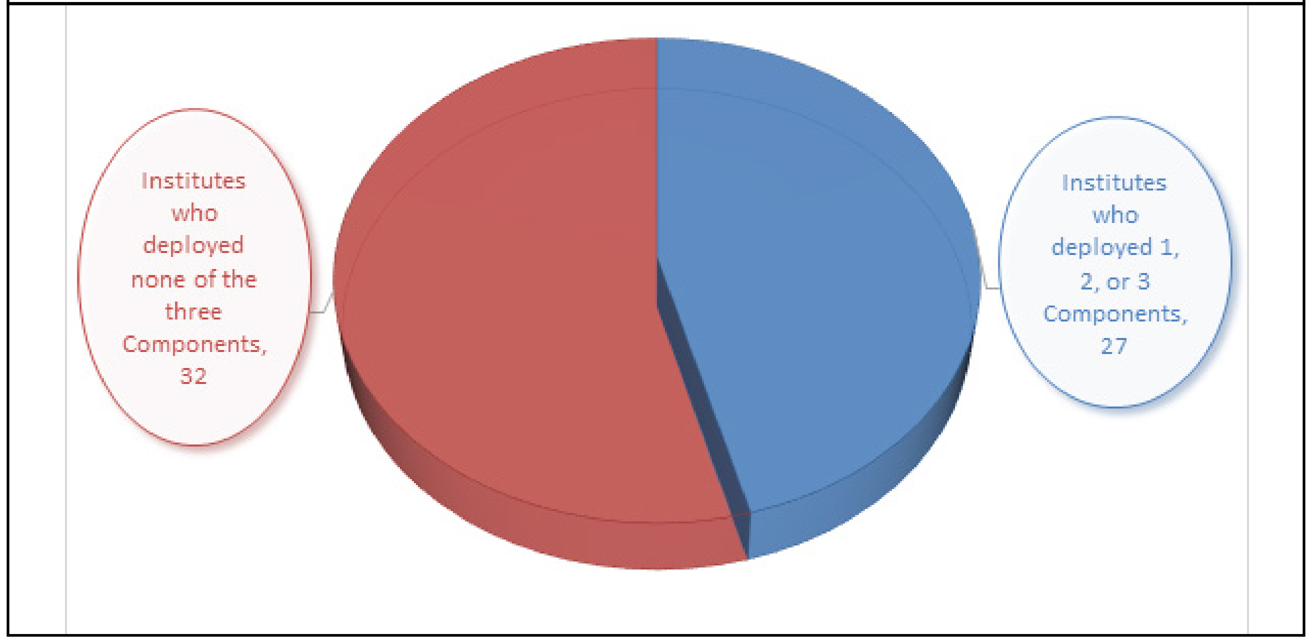


Table 2
Individual Deployed Component

Total Number of Institutes	Education		Training		Awareness	
	Yes	No	Yes	No	Yes	No
59	17	42	18	41	26	33
	29%	71%	31%	69%	44%	56%

Table 3
Categories Deployed By Component

Number of Components Deployed	Number of Institutes
3	17
2	17
1	27
0	32

Table 4
Distribution of the
Deployed Individual Component

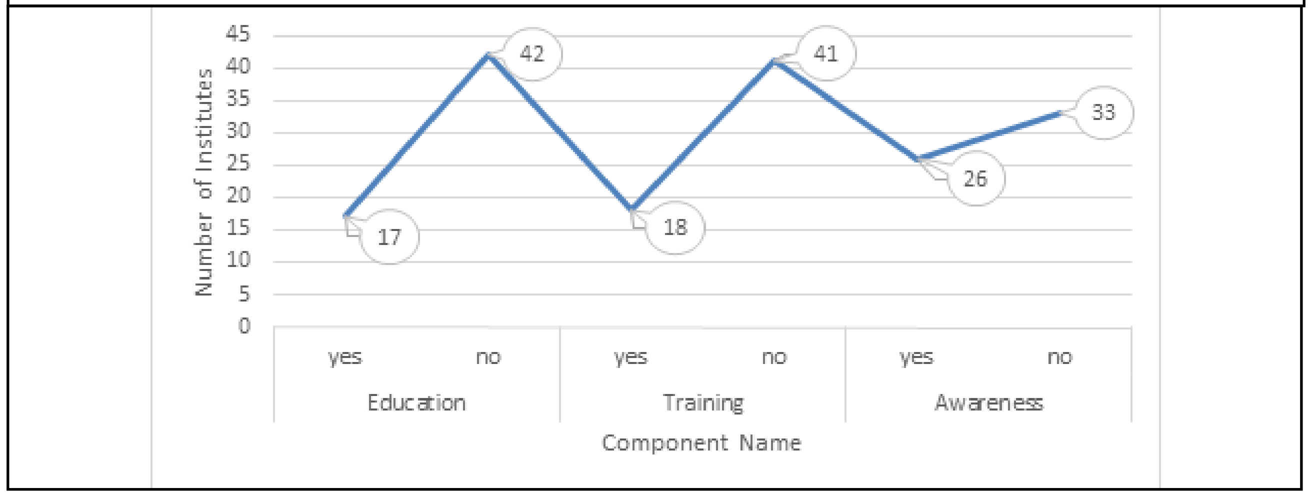
Components Deployed	Number of Institutes
Education, Training, & Awareness	17
Training only	1
Awareness only	9
Total	27

INTERVIEW DATA ANALYSIS

Based on the findings from the preliminary websites examination, five questions were asked during each interview to solicit the interviewee's opinions in regard to the causes of inadequate implementation of the *InfoSec* program. Specifically, the interview questions were:

1. What are the most critical issues facing information security executives to implementing *InfoSec* program?
2. What is the impact of absence of *InfoSec* program in raising security issues among your campus community members?
3. How much agreement is there between the information security professionals and the top management administrators about the importance of deploying *InfoSec* program?
4. Did you have formal training in information and system security? Have employees received adequate training to fulfill their security responsibilities?
5. What is the impact of the cultural practices on the success of information security program?

Figure 2
Individual Deployed Component



The responses of the interviews showed the top three main reasons for lacking the *InfoSec* program in place. Among the top three main reasons, 94% of the participants revealed insufficient level of knowledge and practices in the *InfoSec* program of information security and IT Staff that qualified them to conduct in-house training or initiated an effective awareness program. Followed by 91% of the interviewees agreed that staff and management managers resisted changes, in particular, related to information technology software, tools, and policies. Finally, 81% of the interviewees revealed that there was no support from the top management administrators to initiate *InfoSec* program.

Although the issues of insufficient knowledge, resistance of change from the staff members, and lacking administrators' support were challenges faced among the institutes examined, almost all (98%) of the interviewees agreed that it was vital and urgent to deploy the *InfoSec* program immediately to prevent potential vulnerability caused by the lack of protection. Furthermore, the interviewees unanimously agreed that the top management administrators' support will play a focal factor in initiating a standard for having *InfoSec* program in place.

NEED FOR ADMINISTRATORS SUPPORT AND OVERSEE

Higher Education Institutes are adopting *InfoSec* program to reduce risks that caused by having too many users connected to the same network including students, faculty, staff, administrative, alumina, parents, and community members. For example the majority of organizations in their websites show information on policies and guidelines, computer and network security, virus alerts, and other computer security awareness information which comply with specific guidelines that align with the organizations' missions and goals. This approach facilitates the way of utilizing organizations resources for all types of users and reduces potential internal and external related security incidents. In turn it will save resources, reduce carry cost, and utilize working time which in turn they are significant factors for improving an organizational performance (Reinhardt, R. (2014).

Having a workforce that is educated and more aware of security areas is like expanding the Information Security department into the whole company. Also it gives the security managers a broader base of brainpower in which they can tap if needed. In other words, instead of having a group of staff trying to secure a specific organization's asset against internal and external threats, it has everyone in the organization looking out for the security interests of the organization. Stephanie D. Hight (2005), stated that if an organization can make people aware of their surroundings, both physically and electronically, it can help the organization to defend against the known and hidden threats.

It is very common for organizations to underestimate the consequences of security transgression especially on today's organizations that involve online transaction via mobile devices and wireless connections. Therefore, many organizations require high standards in employee's training and education, also they implement and strictly enforce policies that help protect organization' information (Vacca, 2009; Eyadat, 2015). Administrators should acknowledge that employees are the first line of defense in the organization since they have an access to the most crucial company information and systems and know how to distinguish between normal patterns and unusual activity. Consequently, no one is better suited to protect company information, than they are; therefore, their training and awareness should be the main focus when it comes to information security.

The great effort of the administrators in deploying *InfoSec* program will empower the top level management to best utilize and save invaluable resources including time and money. Also it improves the ability of the employees to acquire the required knowledge, skills, and awareness to properly perform their tasks which is vital for an organization to be competitive and enhance its performance (Vacca, 2009).

In summary, top management administrators should support and work together with the information security professionals to assure that a successful *InfoSec* program is in place. Moreover, administrative should strongly support the idea of integrating *InfoSec* into their strategic management model, so to be more effective and then enhance organizational information management and performance.

CONCLUSION AND RECOMMENDATIONS

The security of institute information systems could be enhanced through *InfoSec;* specifically, education and training on the issues of security lead to the improvement of security awareness. The increase of the knowledge on security issues provides a better practices to the institute's community members, which in turn protects the system resources.

This research highlighted the importance of the administrators' roles in deploying *InfoSec* program and examined the current status of the *InfoSec* program employed by the Saudi Arabian higher education institutes. The research also discovered an alarming and troublesome low rate of having *InfoSec* program in place. The results indicate that 81% of the interviewees revealed that there was no support from the top management administrators to initiate a partial or full *InfoSec* program this led to the other finding which is a high percentage (56%) of the examined institutes offer no *InfoSec* program and only 44% offer a partial *InfoSec* program. The results are aligned to the literature survey findings. A review of the literature in the arena of information security within higher education communities shows a high percentage of lacking in the adequate knowledge and practices of *InfoSec* program due to the unavailability of such program in most of the higher education institutes (Marks & Rezgui, 2009; Androulidakis & Kandus, 2011; Chan, & Mubarak, (2012)).

Due to the rapid evolution of the technologies, the popularity of online learning, and the unawareness of the *InfoSec* program led to an increase in potential threats that could leave the institutes' resources and assets at risk. Thus, to avoid the potential threats that may cause the damage or loss of institutes' data and information, the management should provide the end users with the opportunity to acquire the essential information security knowledge and to receive proper training through the *InfoSec* program. The *InfoSec* program is an essential part of defending information system security and it offers the chance of communicating with the users in regard to the organization's information system policies. In summary, an information system without *InfoSec* program is vulnerable and prone to be hacked.

It is, therefore, recommended that a higher education institute should offer a formal *InfoSec* program, a key factor to the successful use of IT resources, to keep their educational environment secured. It is also recommended that administrators should assure that the *InfoSec* program includes a clear ethical policy and a strong restrictions that are in place. In addition, they should incorporate clear definitions of user responsibilities for information security. Furthermore, an institution must conduct follow up information security 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.

RESEARCH LIMITATIONS AND FUTURE RESEARCH

The study focused on one country and this may limit its generalization. Therefore, by including other institutes from different countries and in the same region. This could reflect different *InfoSec* programs' status. Personal interviews could be increased to include administrators from different levels and different institutes. This could have added invaluable data leads to greater insight into the participants' thoughts and opinions. A standard framework for an effective *InfoSec* program that aligns with the religion, culture, and regulation of that region could be established through further research

REFERENCES

Ally, M. (2009). *Mobile learning transforming the delivery of education and training*. Edmontona: UA Press.

Androulidakis, L. & Kandus, G. (2011). What university students do (or don't) know about security in their mobile phones. *Telfor Journal, 3(1).*

Androulidakis, L., & Papapetros, D. (2008). Survey findings towards awareness of mobile phones' security issues. *Proceedings of the 7th WSEAS International Conference on Data Networks, Communications, and Computers.*

Banerjee, D., Cronan, T., & Jones, T. (1998). Modeling IT ethics: A study in situational ethics, *MIS Quarterly* 22(1), 31-60.

Bere, A. (2013). Using mobile instant messaging to leverage learner participation and transform pedagogy at a South African University of Technology. *British Journal of Educational Technology.* 44(4), 544–561.

Chan, H. & Mubarak, S. (2012). Significance of Information Security Awareness in the Higher Education Sector. *International Journal of Computer Applications,* 60(10), 887–975.

Eyadat, M. (2015). Information security SETA program status at Jordanian Universities" *Journal of Information Privacy and Security (resubmitted on April. 2015)*

Eyadat, M., & Al Sharyoufi, R. (2014). Students awareness toward mobile wireless technologies security issues at college of computer science & computer engineering-Taibah University. *The Journal of International Management Studies,* 14(3), 35-46.

Fatani, H.A., Zamzami, I.F., Aydin, M., & Aliyu, M. (2013, March). Awareness toward wireless security policy: Case study of International Islamic University Malaysia. *Information and Communication Technology for the Muslim World (ICT4M), 5th International Conference.* 1 – 5.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics* 60(2), 151-157.

Gurman, B. & Roback, E. (1995). National institute of standards and technology, an introduction to computer Security: The NIST SP800-12.

Herold, R. (2010). *Why Information Security Training and Awareness Are Important, Information Systems Security, Auerbach Publications, New York.*

Katz, F. (2005). The effect of a university information security survey on instructing methods in information security. *Proceeding on Information Security Currculum Development*, 43-48.

Kim, S.H., Mims, C., & Holmes, K.P. (2006). An introduction to current trends and benefits of mobile wireless technology use in higher education. *AACE Journal, 14*(1), 77-100.

Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & security,* 27, pp. 224–231.

Lockstep Consulting, (2004). A Guide for Government Agencies Calculating Return on Security Investment, Version 2.0, 13 June, https://www.finance.nsw.gov.au/sites/default/files/ROSI%20Guideline%20SGW%20(2.2)%20Lockstep.pdf (Accessed, August, 2014)

Marks, A., & Rezgu, Y. (2009). A comparative study of information security awareness in higher education based on the concept of design theorizing. *IEEE*. 1-7

Reinhardt, R. (2014). Improving Organizational Performance by a Knowledge Related Measurement- And Monitoring-System. *Business and Management Studies, Management Center Innsbruck. Austria.* http://www2.warwick.ac.uk/fac/soc/wbs/conf/olkc/archive/oklc5/papers/k-4_reinhardt.pdf (Accessed Novber, 20014).

Thomson, M. & Solms, R. (1998). IS security awareness: educating your users effectively. *Information Management & Computer Security* 6(4), 167-173.

Traxler, J. (2007). 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, 2013, from http://www.irrodl.org/index.php/irrodl/article/view/346/875

Vacca, J. R. (2009). *Computer and information security handbook*, Morgan Kaufmann, New York, 2009, p. 249

What is HPT: http://www.ispi.org/content.aspx?id=54 ,(Viewed Number 2014)

Whitman, M. E. & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston: Course Technology.

Whitman, M. E., & Mattord, H.J. (2014). *Management of information security* (4th ed.). Boston: Course Technology.

Wilmoth, F.S, Prigmore, C, & Bray, M. (2002). HPT Models: An Overview of the Major Models in the Field, *International Society for Performance Improvement*, 42(2).

Wilson, M. & Hash, J. (2005). National institute of standards and technology, building an information technology security awareness and training program: *The NIST SP800-50.*