THREATS TO INFORMATION SYSTEM SECURITY IN SAUDI ARABIA SECURITY AGENCIES: A COMPREHENSIVE CASE STUDY

Saleh Al-Zahrani
Dept. of Computer Information Systems
School of Computer and Information Science
Imam Mohammad Bin Saud Islamic University, Riyadh, Saudi Arabia

Abstract

The use of information systems has become a necessity for all types of organizations to perform the day to day functions efficiently. The employees and networked information systems are most valuable assets for any organization. The misuse of Information Systems poses serious challenges to organizations including loss of productivity, legal liabilities and trust.

The main goal of this study is to examine the source of threats to information systems in Saudi security agencies and the likelihood of security incidents and the steps they should take to secure their information. We employed quantitative and qualitative methods, such as questionnaire surveys, group meeting and face-to-face interviews supplemented by a document analysis to obtain rich picture. Findings indicate that there is evidence that threats come from outside the country. This result contradicts with studies in western nations. This requires more studies focusing on information security threats in Saudi Arabia in general and in security agencies in particular. The author believes this study will attempt to fill the knowledge gap in information security and information threats in security agencies in developing nations.

Key words.
Saudi Arabia, Security agencies, Misuse of Information Systems, Insider threats, Information security threats.

1. Introduction

In the information and communication technology (ICT) age as the dependency on the knowledge exchange is increasing, many countries are concentrating on building their own national networks. Saudi government has set programmers to encourage their organizations to implement and use information networks (Al-Zahrani, S. 2006). In fact, some organizations have implemented advanced technology to provide high standards of life. Many security organizations have been linked to exchange knowledge, and citizens' information electronically. As more people, systems, and network goes online, the security threat increases everyday. Many organizations are spending much money and time in attempting to fix security problems. Increasing information security threads lead

the IT to the strategic level planning. Information systems need to be protected from many possible attacks such as computer viruses, trojans, worms, and other debilitating networked-based attacks. The major recent attacks are found to be emerged from the networked systems. Consequently, it is an imperative that technologies be examined. All governments face a variety of threats from a variety of sources, the greatest potential threat comes from insiders with legitimate access to those systems (US A Information Security Report, 2009) (Christian W. Probst and Jeffrey Hunker, 2010) (Anderson, J., and M. Brann, 2000) (Al-Zahrani, S., 2006) (Abu Musa, 2006) (Shahrin. S., et. al. 2007) ((Roland Kaschek, 2007) (Alshenaifi, A., 2007) (Knapp, K. J., et. al. 2007) (Jason Crampton and Michael Huthm, 2010). It is likely that most government insider abuse incidents are not reported (Jatinder Singh, et. al., 2010), (Jason Crampton and Michael Huth 2010) (Christian W. Probst and Jeffrey Hunker 2010) (John D'Arcy, et al. 2010).

Currently, the threats to information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional and intentional, targeted or non targeted, and can come from a variety of sources (US A Information Security Report, 2009).

Security agencies should treat citizens' information as one of the most important assets like employees and money. Literature review indicates that there is a lack of previous studies that addresses the issue in Saudi Arabia, For example (Mohammed Alnatheer, and Karen Nelsony, 2009) (Al-Zahrani, S., 2006). Furthermore, according to researcher' knowledge and experience with security agencies, he observed that some employees are not aware of the information threats and hazards that affect the capacity and efficiency of information systems. The researcher believes that some of them don’t exchange and use citizens' information in confidential and efficient ways. Therefore, examine the sources of threats to information systems and the extent of awareness among officials and employees in the security services agencies was the theme of this study.

The main goals of this study are to assess information systems security and find out where information threats come from. In addition, it also examines employees’ perceptions of security policies, security awareness, and preventative methods. Finally, explore the basic steps that need to be taken to prevent attacks in security agencies.

The study is organized as follows. Section two is the current status and related work followed by data collection and analysis section, followed by results of the study section. Section 5 is actions and procedure relating to the protection of information systems. Section 6 is discussion, and finally section 7 is conclusions.

2- Current Status and Related Work

Currently, many types of threats are facing information systems (Jason Crampton and Michael Huth, 2010) (Claerhout B. and DeMoor, 2005) (Younghee Lee, et al. 2010).

These include: accidents, software errors, hardware failures, or environmental influences such as fire. Each of these threats requires proper planning and control. Malicious threats also cover a wide range of activities, from robbery and physical theft to destruction of property. Threats may be an insider or external to the organization (John D'Arcy, Anat Hovav, Dennis Galletta, 2009). The activity may be from an individual, group, organized criminal elements, corporations, or governments. While the motivation behind criminal threats is important in evaluating risk, any attack against the information infrastructure of a business can cause severe disruption and may result in loss of funds, productivity, market share, or reputation and trust.

Criminal activity against information systems is growing because most organizations moving to computer-based operations (US A Information Security Report, 2009). Moreover, increased connectivity and ineffective security controls allow greater access to information and services while providing anonymity. In addition, cyber intruders continuously monitor vulnerable systems so that they can interrupt services, transmit viruses and damage the system as much as they can. The researcher Shahrin said as a network grows in size and complexity, vulnerabilities within local area and wide area network increase and become more problematic (Shahrin S., et. al, 2007). In addition, popularity of intrusion tools and script also make it easier for anyone to launch an attack to any unguarded machines. Before an attacker is able to compromise a specific machine, valuable information such as IP addresses and vulnerable applications are first gathered. There are numerous techniques to get this information. In order to detect these attacks, introducing intrusion detection system (IDS) inside the network is necessary. IDS has the capabilities to analyze the network traffic and recognize incoming and on-going intrusion.

Several solutions were presented to address the problems of security. For example, Bawazir (2007) claimed that the successful applications for information security solutions is that more than 80% of the efforts should be given to developing the skills of employees and restructuring of the business, while the disposal of 20% of its efforts to technology. This includes awareness, training and certification programs; and might come back to termination and end of contracts. All of these factors work together and state that the implementation of an IT security solution is an ongoing activity.

John D'Arcy, Anat Hovav, Dennis Galletta (2009) find out that insider misuse of information systems resources (i.e., IS misuse) represents a significant threat to organizations where 50%–75% of security incidents originate from within an organization. They present an extended deterrence theory model that combines work from criminology, social psychology, and information systems. The model posits that user awareness of security countermeasures directly influences the perceived certainty and severity of organizational sanctions associated with IS misuse, which leads to reduced IS misuse intention. Philip Woodall, and Pearl Brereton (2010) believe access controls are not sufficient to prevent the release of secret information from an information system

unless they address the problem of inference. An inference strategy is a method by which a user can infer secret information using the information which they are allowed to access through the access control mechanism.

Christian and his colleagues outline the basic steps to prevent insider attacks (2010). They found Insider threats to organizational information security are widely viewed as an important concern, but a little is understood as to the pattern of their occurrence. Many practitioners report that their organizations take basic steps to prevent insider attacks, but do not attempt to address more serious attacks. They suggest that further work needs to be done to understand how to better change underlying motivations of insiders, rather than simply focus on controlling and monitoring their behavior. Like wise Jason Crampton and Michael Huth (2010) found out insider threats pose very significant security risks to IT systems and awareness programs are needed.

In term of use of IT and information systems threats in Saudi organization, IT is needed for rapid economic development. Therefore, Saudi government has paid a great attention to adopt IT in all aspects of organizations. Today a large number of organizations already make extensive use of IT (Al-Zahrani and Al-Ghatani, 2006). Security agencies are of the most important government organizations deal directly with citizens and non citizens information management. One of its functions is to protect citizens and their information against the effects of disasters or threats. Saudi government therefore, should aim to use the most up to date IT technology to protect their citizens information from any threats.

The researcher Al-Zahrani (2006) investigates several issues relating to hospital information systems security in Saudi Arabia. The study indicates that medical and IT staff are aware of consequences releasing patient medical information. This study however reports malicious attacks occur by outsiders. This study contrasts with several researchers in the UK and USA. Western studies report the majority of malicious attacks carried out by insiders.(Amatayakul, M., (1999), (Anderson, J., and M. Brann, 2000), (Claerhout B. and DeMoor, 2005). It was not expected to discover such result but we believe this is because of religious and cultural regulations.

Other organizations, in particular, the financial organizations, are the main target for hackers due to their network infrastructure. Abu-Musa (2006) reported that almost half of the responded Saudi organizations suffered financial losses due to internal and external computerized accounting information systems security breach. The study revealed that accidental and intentional entry of bad data; accidental destruction of data by employees; employees' sharing of passwords; are the most significant perceived security threats to accounting information systems in Saudi organizations. It was recommended to strengthen the security controls over the above weaken security areas and to enhance the awareness of information security issues among Saudi organizations.

Again, Al-Zharani, S. and Pit.Pichappan (2007) Suggested a framework of enabling security systems to improve the security of the nation's critical infrastructure. Their survey has provided an opportunity to review and reflect on broader infrastructure requirements to ensure more security for the systems. Security systems can operate at different levels, and every effort needs to be made to ensure that security issues never compromise. In particular, for a system to be made operational under the best possible circumstances, the initial launch of a system must conform to strict quality assurance guidelines. In order to ensure a comprehensive information security policy, they have surveyed the existing security system by using the following variables. They are: Unit testing, Functional/System testing, Environment testing, Data conversion testing, Actuarial certification testing, User acceptance testing, Volume/Stress testing and Version upgrade testing. The use of the above variables ensures an improved security for organizations.

Mohammed Alnatheer and Karen Nelson (2009) have suggested framework for understanding information security culture and practices in the Saudi context. They claimed that an examination of Information Security and Information Security Management (ISM) research in Saudi Arabia has shown the need for more rigorous studies focusing on the implementation and adoption processes involved with culture and practices. Overall, there is a lack of academic and professional literature about ISM and more specifically IS culture in Saudi Arabia. They have identified issues and factors that assist the implementation and the adoption of IS culture and practices within the Saudi environment. Authors believe that there is a gap in terms of addressing the influences of both ISM factors and cultural factors on the adoption of security culture in any Saudi organization.

Finally, we can conclude that, there are several authors have examined IT in Saudi Arabia organizations. However, there is a lack in studies investigating information systems threats. Therefore, we believe this study will attempt to fill the knowledge gap in information systems security and information threats in security agencies in developing nation and in Saudi Arabia in particular.

3- Data Collection and Analysis

The researcher conducted a questionnaire surveys (conducted with participants from three categories), group meeting and face-to-face interviews. The researcher conducted face to face interviews with decision makers such as IT mangers at each site. Each site provides the data such as a basic understanding of each security organization, its mission, and their past risk management activities, their key information assets, highest risk threats, general countermeasures in place, and their prior experience with both successful and unsuccessful attempts involving those threats. Interviews supplemented by a document analysis of activities relating to use of IT security and information threats in security

agencies in Saudi Arabia. Also, direct observations and authors experiences were used to obtain a clear view.

The data collected were coded and processed into a Statistical Software Package (SPSS). (160) questionnaires were distributed in January 2010. Of these, (133) questionnaires were returned giving a response rate of (83.1%). Descriptive statistics were used to characterize the response to each question in the questionnaire. Each question was tested at 0.05 level of significance.

The participants were asked to specify their position. The results showed the majority were military staff (79.7%). Minority were civilians (20.3%). Results indicate that there is diversity in the nature of the respondents. According to aim and functions of security agencies services, the nature security agencies works are based on secrecy and sensitivity. Therefore, it is natural that most of the workers are from the military.

Participants were asked about their highest academic qualifications. The responses were grouped into four classes. Table (1) shows that the majority of respondents (42.9 %) possess high school diploma, followed by university degree (38.3 %) and (9.8) had obtained a master's degree or above. Only (9%) of respondents had less than high school. As a result, there are diversity of the educational level of the respondents. This means that the identified information systems threats in the security services will be affected to some extent by their background. This result indicates that security agencies need to raise the educational level of some of its employees.

Qualification	Frequency	Percent (%)
Less than high school	12	9
High school	57	42.9
Bachelor degree	51	38.3
Master degree or above	13	9.8
Total	133	100

For the purpose of this study, the respondents were grouped according to their age into four classes. They were asked to specify their age group. Most respondents (47.3 %) were aged between 25 and less than 30 years old, followed by (22.6 %) aged from 35 and less than 40. Table (2) shows that majority of respondents have good experience which could be utilized to improve IT role for making decisions regarding information system security. Those who less than 30 years need more training courses in the field of information systems security.

Table 2: Respondents by age

Age	Frequency	Percent (%)
From 25 to less than 30 years	63	47.3
From 30 to less than 35 years	28	21.1
From 35 to less than 40	30	22.6
From 40 to less than50	12	9.0
Total	133	100.0

Also, statistical results indicate that Chi square was statistically significant at level of 0.01 or less, which shows the different views of the respondents.

4- Results of the Study

To analyze the results of the study, the researcher analyzes the responses, addressing the analysis of sources of threat and determine the extent of awareness of staff. Statistical analysis were used to determine, average, mean, and standard deviation. Chi square test at level of 0.01 or less, was used to shows if there is a statistically significant different of the respondents views.

To achieve the main goal of this study, target audiences were asked to identify the sources of information system threats. They have agreed on the importance of identifying different sources of threats. The first question of our study was to determine what source of threats to information systems in security organization (94.7%) of respondents identified the most important source of threat to information systems come from external source, whereas the minority (5.3%) report the most important threat from internal. Its amazing that these results contrast with studies conducted in western nations. For example, (Jason Crampton and Michael Huth, 2010) (Christian W. Probst and Jeffrey Hunker, 2010). On the other hand result in this study agreed with Al-Zahrani.S, (2006).

Statistical results indicate that Chi square was statistically significant at level 0.01 or less, which shows the different views of the respondents to the source of threats.

The respondents were asked to rank the most important reasons for information threats to information systems in security agencies. Several reasons were listed but respondents ranked the most important reasons. One of the most overlooked threats in security agencies is the threat posed by employee behavior. Some staff neglects to keep a password, came in the first place (81.2%). No matter how good business procedures, people used to make mistakes. Managers and staff forget to log off, do not change their passwords, or neglect to have the latest software because they are too busy. Agencies have experienced a wide range of incidents involving data loss or theft underscoring the need for improved security practices. The survey results reveled that the loss of storage media, is a close second in perceived threat level (83.4%). These problems have led

government officials to become increasingly concerned about the potential for losing data. It is a common practice in the developing countries that people do not respect copyright. Unauthorized copying of files to portable storage devices is on of the most serious threat and a major source of information leakage from organizations. It was ranked as third reason (78.9%). However, inadequate security procedures and security measurements ranked as fourth reason (75.2%). Although, many types of conversations may be subject to electronic eavesdropping, stolen and spy on the organization's information, came as fifth reason (70.7%). Data protection is an essential legal requirement for all organizations. Nevertheless, modify data, change data or delete it, rated as no six (70.7%). The use of (IT) is subject to various kinds of potential risks, for example, natural disasters such as earthquakes, rain, rated as seventh reason (69.1%). Finally devices and equipments theft, came as the last reason of information threats (62.4%).

In light of this results we can conclude that these results are consistent partially with the findings of study conducted by Alabodi (2003) as well as with the study of Schultz, E. (2004) which indicate that inadequate security procedures, and modify data, change and delete were the most important threats to information systems. Also, lack of ability to maintain storage media lead to the loss of data.

The study shows the importance of awareness of the consequences of giving information to non-authorized persons. This is confirmed when the majority of staff (94.7%) were aware of the consequences of giving information to unauthorized, while minority (5.3%) were unaware of the consequences of passing information to unauthorized. The majority of respondents view the use of business emails for personal matters as a moderate or major threat, but around third does not address this behavior in their acceptable use policies or make any attempt to deter it. All security agencies report widespread violations of corporate policy. These results agrees with (Al-Zahrani, S., 2006).

During each interview, we obtained a basic understanding of each security organization, its mission, and their past risk management activities. Respondents identified their key information assets, highest risk threats, general countermeasures in place, and their prior experience with both successful and unsuccessful attempts involving those threats.

The sharing of passwords with work colleagues or family members is one of the awareness issues that it needs more attention. Literature revealed that most current systems utilize passwords for authentication purposes. Passwords have often been shared or even recorded on or close to the computer terminals.

Respondents were asked about the exchange of passwords with colleagues at work or give it to a family member. There is evidence that (90.2%) did not give the password to work colleagues or a family member. People used to make mistakes, in fact (7.5%) rarely

give it while the minority (2.3%) is usually given to the work colleagues or a family member.

The study showed that there is no sharing of passwords, or guessing of passwords and great portion of staffs don't share their password with others.

Staff should be aware that their password may be guessed or "cracked" if he or she choose a common word, or their nickname, or the name of their favorite team. They should choose a password that combines letters, numbers, and special characters. They should be informed that it is their responsibility to keep them secure and to not share it with others. This finding is consist with most previous studies. (For example, Abu-Musa, (2006), K.V. Renaud (2009), Mohammed, Alnatheer and Karen Nelsony. (2009).

5- Actions and Procedures Relating to the Protection of Information Systems:

Users need to be aware of the likelihood of security incidents and the steps they should take to secure their sites. Many actions were presented to maximize staff awareness towards information systems threats. They are:
A- Protect devices and keyboards from access by visitors and non-users come first (98.5%) as important action to protect information.(IS).
B- Unauthorized access to the computer rooms came in second position (96.2%).
C- Educate staff, especially the new ones on the penalties for misuse of systems and programs came in third place (95.5%). Therefore, each security agencies should develop clear rules for staff so that they understand what they need to be aware of and their responsibilities. Also, they should have clear policies on personal use and what is, or isn't, allowed. In addition, more awareness tainting programmers among workers and set up security policy are needed.
D- Make staff aware of risk if they share their password with colleagues or a family member (96.3%). Its important to insure that only selected users or groups (based on their responsibilities, privileges, and need-to-know) are allowed access to certain data. The study showed that the final procedures is to recognize the danger of passing information to others where (94.7%) of responds were aware of this procedure. Study provide evidences that staff agree that the success of IS security depends partially on the effective behavior of the individuals involved in its use.

It is very important to prevent entry of unauthorized to the rooms of the systems. They should consider taking into account the confidentiality and privacy of information when it is sent to another party. IT staff, especially those new should be educated to be aware of penalties for the misuse of systems. Also, staff should work with caution when they exchange information concerning the work with others giving more attention to actions and procedure expresses the awareness of staff in the security agencies.

These results are consistent with the findings of the study conducted by (Al-Zahrani, S. and Pit Pichappan (2007), Steyn, Ha Kruger, and L Drevin (2006), Mohammed Alnatheer and Karen Nelson (2009) which concentrated on the importance of increase awareness of sources of threat to protect information systems. Also agrees partly with the findings of Alabodi (2003). The finding also consistent with (Al-Zahrani, S. (2006). He focused on the importance of educating workers information privacy as a means to avoid the sources of threat at different level. Moreover, the finding also, consistent with several studies such as (Chang, S. , E., Lin, C. 2007) (Chen, C., et. al. 2008) (Hong, K., Chi, et. al. 2006) (Hong, K., Chi, et. al. 2003) (Sokratis, et. al. 2010) (Younghee Lee, et. al., 2010) (Thomson, K., et. al. 2006).

T-Test showed that it is not statistically significant at the level of significance (0.81). There is agreement in the views of the respondents on the level of awareness on information systems threats. Also, there are no differences between the military and civilian personnel in the level of awareness regarding information threats.

6- Discussion

The findings of this study indicated that the staffs agreed that there are several threats facing them every day. They strongly agreed on the training programs require to manage a crisis that may face as result of attacks. The findings of this study confirm that there is a strong agreement on the importance of awareness. Most organizations view security threats as inbound from outside to inside. The finding indicate that there are two source of threats, internal and external, however, the external is more aggressive. In fact, internal threats can be employees, contractors, service providers, or anyone with legitimate access to a system. All internal users have some degree of physical or administrative access to IS. The greater access to the system, the greater the potential threat from that person, with individuals having privileged access posing the greatest potential threat.

The Study find out that main threats come from outside. This result is conflict with result of Western studies. (Amatayakul, M., (1999), Anderson, J., and M. Brann, (2000), Claerhout B. and DeMoor)2005). Saudi agencies like other suffering of a number of security problems. For example, Sanjay Rawat, Ashutosh Saxena (2009) believe that in the last few years have witnessed a rapid growth in information attacks, with daily new vulnerabilities being discovered in computer applications. Various security-related technologies, e.g., anti-virus programs, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPSs), firewalls, etc., are deployed to minimize the number of attacks and incurred losses. However, such technologies are not enough to completely eliminate the attacks to some extent; they can only minimize them.

Usually users need to be aware of the likelihood of security incidents and the steps they should take to secure their sites. It is advisable to identify the specific threats against which protection is required. However, there are many actions that must be taken in the

security agencies in Saud Arabia. Information security policy go well with finding and contribute to the nature of the work of security agencies which are based on secrecy and sensitivity. Among them is to establish a unite for information security to monitor and implement information security policies and penalties on violators in security agencies is needed.

T-Test show that it is not statistically significant at the level of significance (0.81). There is agreement in the views of the respondents on the level of awareness on threat Also, there are no differences between the military and civilian personnel in the level of awareness regarding information threats.

7- Conclusion

The main goal of this study was to examine source of threats to information systems in Saudi security agencies and the likelihood of the security incidents and the steps they should take to secure their information.

The number and seriousness of information security problems over the past years indicates that organizations are more vulnerable than ever. However in Saudi security agencies there are major threats to security that are come from external sources. These results contrast with most studies in western nations. Results provide that security policies, security awareness education/training, computer monitoring, and preventative security software are each effective mechanisms for deterring employee misuse of IT resources. These countermeasures should be considered as a group in order to be effective. Employees must also be made aware of security countermeasures for them to be effective. Security policies can be introduced during employee orientation sessions. Security awareness programs, for example, build upon a clear set of security policies and procedures that have been put in place should receive support from top management.

Saudi security agencies are advised to develop contingency plans for scenarios with much lower probabilities such as earthquakes, hurricanes, or other natural disasters; they should develop proactive plans on how to deal with malicious insider threats as well. Finally, is interesting to recommend to conduct a comparative study on the issues related to information security such as confidentiality, privacy, source of threats, and the impact of information exchange between the Western and Muslim countries to determine the effect of religious values and social customs on the behavior of workers in information systems field.

References

1) Abu-Musa, Ahmad A. “Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations,” J. King Saud Univ., Vol. 18, pp. 1-26, 2006.

2) Alabodi. Saad. Proposal of new approach for assessing the maturity of information security in Saudi organizations. Master thesis. University of Hull. May 2003.
3) Alshenaifi ,A. Catastrophic Terrorism and Intelligence. The Information Technology and National Security Conference.1-4 December(2007),. pp 642-759. Riyadh. Sa
4) Al-Zahrani S. and Al-Ghatani, Y., "Empirical Investigation of End Users Attitudes Towards ICT in Saudi Arabia," Proceedings of the 4th International Multiconference on Computer Science and Information Technology, CSIT2006, Amman, Jordan, University press. Apr. 5-7, 2006, pp. 124-129.
5) Al-Zahrani,S. , Awareness of Hospital Information Systems Security: Perspective from King Saud University Hospitals .Information Security Symposium, Taibah University. College of Computer Science and Engineering. May 22-26, 2006 :pp 159-17.
6) Al-Zahrani,S. and Pit. Pichappan ,An empirical study of 'enabling security systems' for organizations: The Information Technology and National Security Conference.1-4 December(2007). PP 1222 -1248. Riyadh. Sa
7) Amatayakul, M., 1999. Security and privacy in the health care information age. MD Computing, 16. (6), 51
8) Anderson, J., and M. Brann, 2000. Security of medical information: the threat from within. MD Computing, 17(2), 15-1
9) Bawazir ,The Key Factors of Successful National Security E-Government in Saudi Arabia as an Example. The Information Technology and National Security Conference.1-4 December(2007),.pp2592-2611. Riyadh. SA.
10) Chang, S., E., Lin, C. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.
11) Chen, C., C., Medlin, D., B. and Shaw, R., S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), pp. 360-376.
12) Christian W. Probst and Jeffrey Hunker(2010). The Risk of Risk Analysis And its Relation to the Economics of Insider Threats. Economics of Information Security and Privacy, 279-299, DOI: 10.1007/978-1-4419-6967-5_14
13) Claerhout B. and DeMoor 2005.Privacy protection for clinical and genomic data. International Journal of Medical Informatics .74 (2-4), 257-265.
14) Da Veiga, A., Martins, N., & Eloff, J.H.P. (2007). Information security culture – validation of an assessment instrument. Southern African Business Review, 11(1), 147-166.
15) Hong, K., Chi, Y., Chao, L., & R., Tang, J. (2006). An empirical study of information policy on information securityelevation in Taiwan. Industrial Management & Data Systems, 106(3), 345-361.
16) Hong, K., Chi, Y., Chao, L., R., Tang, J. (2003). An integrated system theory of information security management .Information Management & Computer Security, 11(5), 243-248.

17) Irvine, Cynthia E.,(2000) "Security Issues for Automated Information Systems," Handbook of Public Information Systems, ed. D. Garson, Marcel Dekker, Inc., New York, NY, pp. 231-245.
18) Jason Crampton and Michael Huthm, (2010). Towards an Access-Control Framework for Countering Insider Threats. Advances in Information Security,, Volume 49, 173-195, DOI: 10.1007/978-1-4419-7133-3_8.
19) Jatinder Singh, Savita Gupta, and, Lakhwinder Kaur,(2010).A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN. International Journal of Computer Science and Information Security, IJCSIS, Vol. 7, No. 1, pp. 284-291.
20) John D'Arcy, Anat Hovav, Dennis Galletta (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research. Volume 20 , Issue 1 .Pp: 79-98.
21) K.V. Renaud (2009) , Guidelines for designing graphical authentication mechanism interfaces, International Journal of Information and Computer Security . Vol. 3, No.1 pp. 60-85.
22) Knapp, K. J., Marshall, T.E., Rainer, R.K. & Morrow, D.W. (2007). Do Information Security Professionals and Business Managers View Information Security Issues Differently? . Information System Security, 16, 100-108.
23) Mohammed , Alnatheer and Karen Nelsony. Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context. Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009, p 6.
24) Olenski, Jozef (2009), The Citizens' Right to Information and the Duties of a Democratic State in Modern IT Environment. International Statistical Review. Volume 71, 33-48.
25) Philip Woodall, Pearl Brereton (2010).A systematic literature review of inference strategies .International Journal of Information and Computer Security. Vol. 4, No. 2 pp. 99-117.
26) Roland Kaschek, A decision making aid for attack response creation. The Information Technology and National Security Conference.1-4 December(2007), Riyadh, Saudi Arabia, pp. 9-60.
27) Sanjay Rawat, Ashutosh Saxena(2009).Application security code analysis: a step towards software assurance. International Journal of Information and Computer Security. Vol. 3, No.1 pp. 86-110
28) Schultz, E. (2004). Security training and awareness, fitting a square peg in a round hole. Computers & Security, 23(1), 1-2.
29) Shahrin Shahib , Asrul Hadi Yaacob and, Mohd Faizal Abdollah , Towards Early Detection of Network Intrusion. The Information Technology and National Security Conference.1-4 December(2007), pp 1049-1062. Riyadh. Sa.
30) Sokratis Katsikas, Javier Lopez and Miguel Soriano, Trust, Privacy and Security in Digital Business. Proceeding of the 7th International Conference, Trust Bus 2010, Bilbao, Spain, August 30-31, pp. 54-62, 2010.

31) Steyn, T , Drevin, L., and Kruger, H.A. Value-focused assessment of ICT security awareness in an academic environment, In: IFIP International Federation for Information Processing, Volume 2, pp. 448-453, 2006.
32) Thomson, K., von Solms, R., and Louw, L. (2006). Cultivating an organizational information security culture. Computers& Security 10, 7-11, pp. 12- 20.
33) USA INFORMATION SECURITY Report(2009). Cyber Threats and Vulnerabilities Place, Federal Systems at Risk. United States Government Accountability Office May 5, 2009.
34) Younghee Lee, Jinkyung Kim, Junghwan Kim, Jiyong Kim and Il Moon, Development of a risk assessment program for chemical terrorism. Korean Journal of Chemical Engineering.Vol. 27, No 2, 399-408, 2010.