IBIMA Publishing
Journal of Innovation & Business Best Practice
http://www.ibimapublishing.com/journals/JIBBP/jibbp.html
Vol. 2016 (2016), Article ID 329374, 24 pages
DOI: 10.5171/2016.329374

Research Article

Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University

Adel Ismail Al-Alawi[1], Sulaiman M.H. Al-Kandari[2] and Refaat Hassan Abdel-Razek[3]

[1]College of Business Administration, Department of Management and Marketing, University of Bahrain, Kingdom of Bahrain

[2]College of Sahria and Islamic Studies, State of Kuwait

[3]Department of Industrial Engineering and Engineering Management, College of Engineering, University of Sharjah, United Arab Emirates

Correspondence should be addressed to: Adel Ismail Al-Alawi; adel.alalawi@gmail.com

Received date: 4 January 2016; Accepted date: 14 January 2016; Published date: 24 August 2016

Academic Editor: Basel M. Al-Eideh

Abstract

The purpose of this study is to evaluate the levels of knowledge, attitude, and behavior of the end-user regarding Information Systems Security Awareness (ISSA) in higher education, specifically Kuwait University (KU), and to identify the areas which require attention. Factors such as knowledge, attitude and behavior affecting human awareness were identified and the Value-Focus-Thinking was used to identify Information Systems Security (ISS) focus-areas. The six ISS Focus-Areas were obtained such as commitment to ISS policy; effective use of passwords; safe usage of Internet and e-mail; being aware of ISS threats; backing up the important files; and required updates for operating system and antivirus programs. Furthermore, a questionnaire was designed based on the human awareness factors and the ISS focus-areas. The research population included the end-users of KU colleges. The study presents useful results for decision-makers in the field of ISS, to identify recent findings regarding the level of ISSA among end-users, and in order to develop better strategies to implement the required solutions such as training programs. In addition to the organizations, this study through concentrating on ISSA may assist individuals to protect their personal data privacy during their use of computers. The study recommends few relevant actions to improve the long term levels of knowledge, attitude and behavior, with the priority for improving attitude due to its identified poor level. Regarding the KU colleges, the study recommends giving priority to improvements to the seven colleges that had poor levels of ISSA.

Keywords: Awareness Factors, Knowledge, Attitude, Behavior, Value-Focus-Thinking

Cite this Article as: Adel Ismail Al-Alawi, Sulaiman M.H. Al-Kandari and Refaat Hassan Abdel-Razek (2016)," Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University ", Journal of Innovation & Business Best Practice, Vol. 2016 (2016), Article ID 329374, DOI: 10.5171/2016.329374

Introduction

Information is considered as lifeblood and a backbone for most institutions, and an invaluable asset in today's IT-enabled world (Al-Alawi 2011, Thomson and Solms, 2006). Therefore, when dealing with Information Systems (IS) for the different institutions, maintaining Information Systems Security (ISS) among the employees, in the form of Information Systems Security Awareness (ISSA), is extremely important to protect the institutions' IS. Concerning the universities, protecting personal information for students and employees is crucial in applications regarding student information system, employee information system and other applications such as financial applications (Drevin et al, 2007, Al-Alawi & Hafedh, 2006). Rezgui and Marks (2008) have stated that ISSA is extremely critical in protecting the universities' assets from knowledge and information to avoid the potential loss.

The various technologies related to IS became important for the different institutions. Although the new technologies deliver a number of benefits, they also introduce new vulnerabilities. The technologies can be exploited unethically by some technically skilled persons, to be acting as hackers, representing the well-known threat for ISS. Hacking IS networks can take place by the use of special programming tools for attacking and hacking, to create and distribute the different kinds of hidden harmful programs, such as computer viruses and hidden Trojan in IS networks. The human errors and the lack of ISSA regarding the use of the technologies related to the organizations' IS network may accidently cause information damage or loss. According to Whitman and Mattord (2004), employee's errors are classified among the top threats to ISS. They also have added that the best way to protect an organization's ISS is to increase and enhance the end-users' ISSA.

The literature showed topics regarding ISSA, but there is no clear and precise published work that provides a system capable of evaluating the level of ISSA at KU, showing a lack of relevant previous studies. Therefore, it is important to conduct further research about ISSA at KU, to better understand what factors are involved, what approaches are applied and other issues related to the study subject. This study may help those institutions, including the universities, who are relying mainly on technical protecting tools such as anti-virus programs and firewalls, to think of strategies that help them to explore the effects of human factors on their institutions. It guides to realize some important issues related to the protection of ISS in the organizations such as ISSA.

Kuwait University (KU) was established in 1966, to be the first institution of higher education in Kuwait that contributes in the advancement of the nation, by serving knowledge and learning. Like any modern university, KU utilizes the scientific means and the modern technologies related to Information Systems (IS), to stay up to date with today's world (Kuwait University, 2010). Information Systems Center (ISC) is the facility of KU that supports the enterprise business processes of KU with available information technology. ISC has the overall responsibility of making sure that technological resources and expertise are available to the KU community and has the overall responsibility of making sure that technological resources and expertise are available to the KU community. ISC oversees ISS and related policy issues by practices such as calling for an understanding of technology and security throughout the University community, developing the university Information Systems Security (ISS) policy and pursuing improved ISS processes and procedures throughout the University community. The objectives of this study are to evaluate the levels of knowledge, attitude, and behavior of the end-users regarding ISSA at KU, and to identify the areas of ISSA which require attention and improvement when developing the solutions to raise the level of ISSA at KU.

Adel Ismail Al-Alawi, Sulaiman M.H. Al-Kandari and Refaat Hassan Abdel-Razek (2016), Journal of Innovation & Business Best Practice, DOI: 10.5171/2016.329374

Literature Review

Introduction

In today's world, where the economy had become digital, the different modern organizations moved towards using a high number of different IT as part of IS to meet the business requirements (Singh et al., 2013, Kankanhalli et al., 2003). As the number of IT increases in sophistication and complexity, the number of threats and vulnerabilities that related to the ISS also rises up challenging the organizations in securing their business information (Karyda et al., 2005). Therefore, ISS is considered as a critical issue that has attracted much attention from the researchers in the field of IS (Feng and Li, 2011). Managing ISS requires realizing and understanding many issues and challenges such as threats identifications, technologies that support ISS, and required ISSA that is considered the most important when addressing the issue of ISS (Theoharidou et al., 2005). The purpose of ISSA is to focus attention on ISS, and allow individuals to recognize ISS concerns to respond accordingly (Stoneburner et al., 2002). The strong security culture cannot develop or grow in an organization without an adequate level of ISSA. According to Furnell et al., 1996, ISSA training programs are required when the organization needs to promote ISS standards. Therefore, it is necessary for the organizations to provide training programs that create or increase employees' ISSA level, to ensure that their employees are aware of ISS risks, thereby protecting themselves (Kruger and Kearney, 2006; Veiga and Eloff, 2010; Albrechtsen and Hovden, 2010, Sirma, et al. 2014).

The Information Systems (IS) and the Information Systems Security (ISS)

The development of IS has provided dramatic changes and played an essential role in the progress of the organizations, realized in enhancing the business performance by supporting the business activities such as the managerial, the strategic and the operational activities that rely on manipulating the business information and the use of its associated technologies (Brooks et al., 2002). According to Watson (2007), IS are compound of socio-technical systems: the social part represents the people; the technical part refers to the different technologies related to IS. Turban et al. (2015) have stated that after a series of developments and innovations had been done in the field of IS, some technological part became computer-based and so called IT, which involves hardware, software, databases, networks, and other electronic devices; considered as a system or a subsystem of IS; and used interchangeably with IS. Since most of the different organizations adopt computer-based IS to perform the required tasks, the term IS is usually used to refer to computer-based IS, as long as there is no indication about not-computer-based-IS.

The word "security" refers to a state of being free from risk or danger, or to protect and regulate an access control to the assets (Oxford, 2014). The terms: information systems security, information security, and computer security all have the same concept and can be used interchangeably (Rezgui and Marks, 2008). According to (Ross, 1999), computer security can be defined as a system ability to protect information and system resources with regard to data confidentiality and integrity. According to Cornell University Law School (2015), United States Code defined ISS as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide… integrity…, confidentiality…, and availability".

Before moving to the world of IS and the associated technologies, the issue of ISS had started for the protection of the secrecy of the written messages, the telegrams and then for the telephone lines (Dlamini, et al., 2009). Solms (1996) has mentioned that ISS has evolved through three stages. The first stage was in the sixties when there was a concern to ensure the physical security for the facilities such as regarding the circulation of the printouts. The second stage started in the middle of the seventies when ISS was

designed to specific needs of individual organizations. The third stage appeared with the advent of advanced technology, to fulfill the organizations' need of linking their IS resources including IT, and move to complex environments that depend on connected networks.

The modern society is increasingly depending on IS and the related technologies because of the economic returns (Siponen, 2005). As the number of IS technologies is increasing in today business environments, responding to the organizations' needs of improving their competitiveness and overall business performance, the number of ISS threats and vulnerabilities is also increasing creating security challenges and difficulties (Khalfan, 2004). Kankanhalli et al. (2003) have stated that at the time that the new technologies deliver a number of benefits, they can be vulnerabilities that can be exploited unethically by some technically skilled persons, to be acting as hackers, representing the well-known threats for ISS that highly damage IS by coding and distributing the different kinds of harmful computer viruses through the computer networks, as well as using special attacking and hacking software like hidden Trojan software.

Information Systems Security (ISS) Objective

According to NIST, (2004), the objectives of ISS can be summarized in protecting information system resources such as hardware, software, and information as an asset, by providing integrity, confidentiality and availability of business information. The integrity of information resources requires maintaining the accuracy and the comprehensiveness of the information (Humphreys et al., 1998). Ritchie and Brindley (2001) have stated that the importance of information integrity plays a major role in the process of decision making; while inaccurate or incomplete information would stray the organization management in taking the required right decisions.

The confidentiality of information requires that the information as an asset needs to be kept secret, and not to be available or accessed by any person except those who are authorized to access the information. Humphreys et al. (1998) have stated that the confidentiality of the information involves protecting and preserving business information from unauthorized party. Thompson and Solms (2005) have added that preserving the confidentiality of information can be through applying a restricting access to confidential information.

The availability of the information resources requires ensuring that resources such as data, software and hardware are accessible by authorized persons at the right time (Zissis and Lekkas, 2010). Gerber and Solms (2001) have stated that ensuring the availability of the required information at the right time is extremely important, because when the organization cannot get the information at the right time, it may not be able to perform the required operations effectively, which leads to the loss of the chance of gaining the competitive advantage over the others. According to Ryan and Ryan (2006), any one of integrity, confidentiality or availability, security objectives regarding information resources, can be compromised by illicit access even if the other two security objectives are preserved.

The Elements of Information System Security (ISS)

From the viewpoint of that the business information is extremely important for most organizations today, the issues such as security for the protection of business information should be extremely important, given more attention, and supported by a lot of efforts (Kankanhalli et al., 2003; Posthumus and Solms, 2004). According to the CNSS (2015), an effective ISS should have the ability to protect IS resources from unauthorized access, whether to the data store system or during data processing or transaction, and to protect from denial of service to authorized users. Posthumus and Solms (2004) have mentioned that addressing an effective ISS in the organization should start from understanding the need for ISS and the consequences of IS abuse, and should be

spanned by the entire ISS environment through educating the employees and defining ISS policy and other related administrative regulations. Proactively addressing an organization's ISS issues in the digital era is not only a good business practice, but it is considered as a necessity.

According to Kankanhalli et al. (2003), the protection of ISS is based on three elements such as technological solutions, human involvement and security policies, while Williams and Andersen (2001) agreed with the previous statement and have added that in order for ISS protection elements to be eligible to function as they are required, the organization should adopt the well utilization of these elements to support the adequate protection for ISS, which can be reached by technological solutions that should be able to detect the security threats, act upon security problems and provide report and by the security policies that should be effectively established and written toward supporting the full meaning of ISS protection, in a well-defined document form. The details of roles and responsibilities have to be clearly articulated and easily available for all employees within the organization.

As for the human element, there should be an adequate awareness evolved by a good security program. When dealing with the different IT among IS, employees from the different administrative levels should have a common level of understanding the requirements of ISS, aware enough about vulnerabilities and threats, and accept their personal responsibilities.

Information Systems Security (ISS) and the Human Involvement

As a concept, ISSA refers to understanding and adopting the optimal practices that insure the commitment of ISS policies toward ISS problems (Siponen, 2005). ISSA is a state of the users' awareness in an organization regarding ISS mission (Rezgui and Marks, 2008). According to Information Security Forum (2003), ISSA is a level of which the organization's employees understand the importance of ISS, their own responsibilities toward ISS and the required actions. Since organizations' success or failure depends on their employees' performance, there should be a high concentration on the employees to be involved in the process of maintaining and protecting ISS (Veiga and Eloff, 2010). Siponen (2005) has stated that organizations' ISS requires focusing on the employees' ISSA by providing the efforts that maintain and promote the level ISSA of the employees. Drevin et al. (2007) have mentioned that the importance of ISSA appears in reducing human error, theft, fraud, and misuse of Information Systems (IS) assets.

Information Systems Security (ISS) at the Universities

Academic institutions face more challenges regarding securing their systems due to the complexity of their Information Systems (IS) (Rezmierski et al., 2002). Maintaining universities' ISS secrecy is extremely important in applications regarding personal information system, research projects and some other applications such as financial applications (Drevin et al., 2007). Rezgui and Marks (2008) have indicated that colleges and universities are targets for attacks because of the high computing power and open access they provide to people within and outside of their institutions. Updegrove and Wishon (2003) have stated that despite the fact that there is always a potential for attacks that breach organizations' ISS, the universities are among the least secured IS, and few of them conduct awareness training.

Information Systems Security Awareness (ISSA)

The term awareness is often considered as a tool for minimizing problems (Al-Alawi, 2014, Thellufsen et al., 2009). ISSA among all kinds of users is extremely important to Information Systems Security (ISS) performance in the organizations (Sirma, et al. 2014, Albrechtsen and Hovden, 2010). Drevin et al. (2007) have mentioned that the importance of ISSA appears in reducing human error, theft, fraud, and misuse of Information Systems (IS) assets. Despite that most of the various organizations are well aware of the importance of ISSA

programs, they are actually not implementing the awareness programs in an effective way that develops and reaches the adequate awareness level that makes their employees capable of dealing with IS safely. Woodhouse (2007) has stated according to a conducted survey that most of ISS incidents in the organizations come from their own employees (insiders), and also many organizations have not conducted any process for evaluating the level of ISSA for the end-users and any training program necessary to insure their ISS.

While information Systems Security (ISS) concentrates on maintaining the confidentiality, integrity and availability of information, ISSA deals with training programs that create and maintain the adequate level for users' ISSA (Kruger and Kearney, 2006). Creating an adequate level of ISSA is extremely important for the users to operate IS securely (Williams and Andersen, 2001). Training can be a solution that creates awareness and prevents employees from accidentally acting inappropriately (Drevin et al, 2007, Offor, & Gurvirender, 2014).

It is very important to implement awareness training program on the entire organization's employees, at all managerial levels of the organization. Management should set examples for proper ISSA in the organization, and perform serious efforts for deploying and implementing awareness training program. The effectiveness of these efforts determines the effectiveness of the awareness training program. The successful awareness training program consists of developing ISS policy that reflects the best practices for protecting ISS, informing employees about their responsibilities toward protecting ISS according to the organization procedures and ISS policy, and processes to monitor and review the program (Wilson and Hash, 2003). Hansche (2001) has suggested that the good ISSA program should be designed with taking in account the following points:

a) The goals and objectives should be clear to all, and the aim should be changing the way people think and act towards security issues.
b) Choosing an appropriate content that addresses the issues about IS threats and vulnerabilities and related solutions.
c) Using different techniques to deliver ISSA materials such as emails, posters, direct training and online training, because the program should have the ability to reach a large audience.
d) Evaluating the program periodically to determine whether the main goals of ISSA were achieved

The importance of Evaluation of the Level of ISSA

Since the employees' ISSA plays a significant role in meeting the objectives of ISS, it is important for the decision makers to conduct an evaluation for the level of employees' ISSA, to deliver a clear picture about the level of ISSA and make sure if employees' ISSA is in the acceptable level of ISSA or requires enhancements (ISACA, 2015). Kruger and Kearney (2006) stated that evaluating the level of ISSA is necessary for ISSA program in adding value to the organization and making a contribution in supporting ISS in the organization. Da Veiga and Elof (2010) have agreed with previous statement and added that evaluating and reporting on the state of ISSA should be done periodically.

The process of evaluating ISSA requires defining two issues. One is related to the human factors to be used for evaluating the human awareness while the other issue is regarding the focus-areas of ISS that should be taken in account for the field of ISSA (Drevin et al., 2007, Offor, & Gurvirender, 2014).

Factors Affecting Human Awareness

Regarding the human aspect, Feldman (1999) has stated that the social psychology field explained that learned predispositions to respond in a favorable or unfavorable manner to a particular thing have three components: affect, behavior, and cognition. The affect component includes a person’s positive and negative emotions toward something; the behavior component is related to the intention that acts in a particular manner; while the

cognition component refers to the thoughts and the beliefs toward a particular thing. The three components were developed on three dimensions equivalently (factors): knowledge (what does a person know about a certain topic), attitude (how does the person feel about the topic) and behavior (what does the person do), to be used for evaluating the human awareness (Kruger and Kearney, 2006). Additional issues and theories, related to human awareness, are presented below:

Protection Motivation Theory (PMT)

According to Rogers and Prentice-Dunn (1997), Protection Motivation Theory (PMT), developed by Rogers (1983), emphasizes that individuals' motivations or intentions to protect them from harm depend on three components: sources of information, cognitive mediating process, and coping modes.

PMT has been applied in many studies regarding predicting users' behaviors, involving the studies related to ISS. Lee et al. (2008) have used PMT model to predict the likelihood of online users' intention to engage in virus protection behaviors and found out that perceived vulnerability to virus threats, response effectiveness of virus protection procedures and self-efficacy were significant predictors of the intention to engage in the relevant behavior. In another study conducted by Pahnila et al. (2007), PMT has been used to determine factors that influence employees' commitment to ISS policy. The study indicated that threat appraisal had a significant impact on the intention to comply with ISS policy. Woon et al. (2005) have also applied the theory to identify factors that influence decision and behavior of the home internet users regarding securing their home network, to test whether threat appraisal and coping appraisal played important roles in making users choose between enabling and ignoring the wireless network security options.

Theory of Planned Behavior (TPB)

Ajzen (1991) has stated that according to the Theory of Planned Behavior (TPB), individuals' behaviors are determined by their intentions, which in turn are influenced by:
Attitude: an individual's attitude toward the behavior.

Subjective norms about the behavior: a person's judgment that people who are important to this person feel that the person should or should not perform the behavior.
Perceived behavioral control: refers to the perception of the constraints of the internal and external resource on the behavior performance.

Gopi and Ramayah (2007) have used the TPB model on a sample of investors and found out that there is a positive relationship between attitude, subjective norm and perceived behavioral control and the behavioral intention of the Internet-users to use online trading. Shih and Fang (2004) have implemented TPB in a study about bank customers. They have found that attitude and perceived behavioral control appeared to be significant predictors of intention to use online trading, while this is not applicable for subjective norm. Lee and Ho (2002) have used the model and stated that attitude and social factors have a significant impact on the intention of the investor towards adopting online stock trading. Athiyaman (2002) has used the TPB and has found out that attitude, social factors and perceived behavioral control have a significant relationship with the user's intention to purchase ticket over the Internet.

Knowledge, Attitudes and Behavior (KAB) model

The Knowledge-Attitude-Behavior (KAB) Model supposes that knowledge influences attitudes which, in turn, control behaviors (Fabrigar et al., 2006 and Hwang et al., 2000).

ABC Model

According to Tipton and Krause (2007) and Martha et al. (2006), ABC model suggests that a person's attitude is based on three rational components:

a) Cognition: the cognitive responses to a particular motivator about the motivator object.
b) Affect: individual's feeling about the object.
c) Behavior: the overt act according to the individual's attitude.

Technology Acceptance Model (TAM)

According to Davis et al. (1989), Technology Acceptance Model (TAM) indicates that an individual's usage of a technology depends on his behavioral intention, which is determined by his attitude toward the usage, which is in turn determined by:

a) Perceived usefulness - the level of a person's belief toward the use of the technology will improve the job performance.
b) Perceived ease of use - the level of a person's belief toward using the technology will save effort.

TAM has been applied in some studies such as in e-banking by Rouibah et al. (2009) and Suh and Han (2002).

Summary of the Human Awareness Factors

Reviewing the literature about studies conducted by: Martha et al. (2006), Fabrigar et al. (2006), Hwang et al. (2000), Lichtenberg and Zimmerman (1999), Rogers and Prentice-Dunn (1997), Ajzen (1991), Kallgren and Wood (1986), has shown that the human awareness factors required for evaluating ISSA can be: knowledge, attitude and behavior. Drevin et al. (2007) have shown the importance of using focus-areas in the evaluation process of ISSA, and how to generate them using technique such as Value-Focused-Thinking (VFT) developed by Keeney(1994). According to Keeney (1994), VFT approach is a decision technique that calls for the stakeholders (decision-makers) to decide "what is important and how to achieve it" by defining what they care about in a specific situation. Table-1 illustrates some personal factors related to the awareness and the relevant studies that explained or adopted these factors.

Table1: Summary of some relevant studies about Awareness Factors

Awareness Factors	The studies
• Cognition • Behavior	Rogers and Prentice-Dunn (1997)
	Lee et al. (2008)
	Pahnila et al. (2007)
	Woon et al.(2005)
• Attitude • behavior	Ajzen (1991)
	Gopi and Ramayah (2007)
	Shih and Fang (2004)
	Lee and Ho (2002)
	Athiyaman (2002)
• Belief	Davis et al. (1989)
	Taylor and Todd (1995)
	Suh and Han (2002)
	Rouibah et al.(2009).
• Affect • Cognition • Behavior	Martha et al. (2006)
• Knowledge • Attitude • Behavior	Drevin et al (2007)
	Fabrigar et al., 2006
	Kruger and Kearney (2005)
	Hwang et al., 2000)
	Lichtenberg and Zimmerman (1999)
	Kallgren and Wood (1986)

According to Table-2, the factors determined are: cognition, behavior, attitude, belief, affect and knowledge. Some of these factors appeared to be overlapped with each other. Kruger and Kearney (2005) have stated that (knowledge) factor can be equivalent for (cognition) and (belief) while the (attitude) factor for the (affect). Therefore, the factors of the human awareness included in Table-2 are summarized in three factors as shown in Table-2.

Table2: Summary of Human Awareness Factors

Human Awareness Factors	1. Knowledge
	2. Attitude
	3. Behavior

The above three human factors, knowledge, attitude and behavior, are used in the current study, for the part related to the evaluation of the awareness.

Research Methodology

Depending on the nature of the study, the methodology employs a case-study approach through KU in the state of Kuwait, qualitative approach using questionnaire as a tool based on Likert-scale technique, and quantitative approach to measure the frequencies.

The research objectives can be broken-down as follows

a)To evaluate the levels of knowledge, attitude, and behavior of the end-users

regarding ISSA at KU.

b) To identify the areas of ISSA which require attention and improvement when developing the solutions to raise the level of ISSA at KU.

Research methodology is designed to achieve the research objectives by the following steps

a) Reviewing the literature for topics and concepts related to the research subject.
b) Identifying the human awareness factors required in the process of evaluating ISSA.
c) Identifying ISS focus-areas regarding KU for the process of evaluating ISSA at KU.
d) Designing a questionnaire form to evaluate the levels of knowledge, attitude, behavior and ISSA of end-users at KU.
e) Analyzing the gathered data and obtaining the results.
f) Setting up and writing the conclusions and the recommendations.
g)

Research Variables and ISS Focus-Areas

The extraction of the literature indicates that the human awareness can be evaluated by the following factors:

1. Knowledge. 2. Attitude. 3. Behavior.

This current study adopts the previous three awareness factors for evaluating the level of ISSA at KU.

Identifying ISS Focus-Areas

The process of evaluating the level of ISSA requires identifying a set of focus-areas related to ISSA according to the target organization. Focus-areas related to ISS at KU have been identified using Value-Focus-Thinking (VFT) approach. There was another approach for defining focus-areas called Alternative-Focused-Thinking (AFT). VFT has been selected in the current study because it provides wider range of alternatives and uses up-to-date information, contrary to AFT (Keeney, 1994). VFT was applied in this study following the steps suggested by Keeney. The steps started with defining ISS-administrators' wishes, and values regarding ISSA at KU. Twelve participants from IS-administrators were interviewed out of more than thirty IS-administrators at KU. They were selected because of their specialty regarding ISS issues. The interviews aim to develop a wish list and identify the alternatives, important to establish values that support ISSA objectives, by asking the following question: What is important to you regarding ISSA of the end-users in your university? Each interview lasted approximately ten to fifteen minutes. The interviews resulted in a set of values regarding ISSA. After the completion of the rest of VFT steps, six ISS focus-areas were obtained as follow.

a) Commitment to ISS policy (FA-1).
b) Effective use of passwords (FA-2)
c) Safe usage of Internet and e-mail (FA-3)
d) Being aware of ISS threats (FA-4).
e) Backing up the important files (FA-5).
f) Required updates for operating system and anti-virus program (FA-6).

Data collection

For the purpose of collecting the required data regarding the level of ISSA of the end-users at KU, a questionnaire was developed depending on the comprehensive survey of the literature in the field of ISSA. The questionnaire consists of two parts as follows:

The first part includes 5 questions that target the personal information of the participant. The personal information includes participant's name, age, gender, years of experience and college name.

The second part includes 36 questions equally distributed on three axes that represent the three awareness factors (knowledge, attitude and behavior). Each axis includes 12 questions that evaluate one of the three awareness factors

according to the six focus-areas defined earlier in this section.

The questions of the first part of the questionnaire are answered by choosing the appropriate answer. The questions of the second part of the questionnaire use 5-level Likert scale.

Validity and Reliability of the Questionnaire

The questionnaire has been judged by a group of arbitrators (academics and practitioners) to check the validity of the questionnaire statements for the field of study, clarity and the easiness as well as to review the quality of the translation into Arabic to be suitable for the research community. The arbitrators' comments and opinions have been taken to modify some statements and then design the final form of the questionnaire. Furthermore, the tool has been statistically tested for validity and reliability, using Pearson's Coefficient of Correlation, and Cronbach's alpha (α) method test respectively. The two tests indicated that the study tool has the acceptable validity and the acceptable levels of reliability to meet these study requirements.

Research Population

The research population is comprised of only end-users of KU colleges, although the colleges include other groups: faculty members and students. The reason for selecting only the staff group is because they are the main end-users of IS resources at KU in their daily activities and responsible for the works that require sufficient level of ISSA. These works are related to the IS of employees, students and other administrative affairs, where the related ISS issues are very important. Whereas, the faculty members and the students have a limited usage of applications related to the university IS. They usually use general applications that are not related to the IS of the university, such as the applications for education or web search engines. Even the groups of faculty members and students should have a sufficient level of ISSA generally; the issue of ISSA of the group of staff is critical regarding the protection of ISS of the university. Therefore, the current study concentrates on the group of staff in the process of evaluating the level of ISSA in the university. In a study related to the evaluation of ISSA in the universities, Rezgui and Marks (2008) conducted a survey using research population comprised of staff.

Research population size is defined according to the staff members that are available during the survey period (June and July). According to the information gathered from the department of administrative affairs at KU, the research population in the current study is comprised of 1076 end-users.

Distribution of the Sample

The questionnaire was electronically distributed using a web-based technique. Invitations for participation have been sent through the end-users' e-mails, via the main Information Systems Center at KU. A formal permission had been granted by the Office of the Secretary General of KU to conduct the survey. It took one month and a half to finish the survey, starting from the first of June 2011 to the fifteenth of July 2011. The number of responses (received questionnaires) reached 317 out of the total population of 1076. But only 303 questionnaires were usable since the other 14 questionnaires were not filled completely or contained conflicting answers. However, the number of accepted responses (303) forms a responding rate of 28%, and is more than the sample size of 284. Table-3 provides breakdown data for all the respondents according to their colleges.

Table3: Respondents Statistical Info According to Their colleges

#	College Name	Population	Accepted Responses	Response Rate
1	College of Law	44	9	20%
2	College of Arts	62	16	26%
3	College of Sciences	166	35	21%
4	College of Medicine	134	32	24%
5	College of Engineering and Petroleum	181	62	34%
6	College of Allied Health Science	56	15	27%
7	College of Education	81	35	43%
8	College of Sharia and Islamic Studies	49	20	41%
9	College of Business Administration	85	23	27%
10	College of Pharmacy	37	11	30%
11	College of Dentistry	31	6	19%
12	College of Social Science	73	17	23%
13	College of Woman	66	18	27%
14	College Of High Education	11	4	36%
Total		1076	303	28%

Data Analysis Procedures

Data analysis is conducted using applications of Statistical Package for the Social Sciences (SPSS) version (19), and Microsoft Office Excel version (2007) software. The first is used for coding and manipulating data, while the second for creating statistical tables and figures.

Regarding the awareness factors, the current study adopted relative weights from previous study. According to Kruger and Kearney (2006), the relative weights for awareness factors are estimated as shown in Table-4, when using knowledge, attitude and behavior as awareness factors for evaluating the level of ISSA.

Table4: Awareness Factors Relative Weights

Awareness factors	Relative Weight
Knowledge	30%
Attitude	20%
Behavior	50%

The relative weights for FA1 to FA6 were obtained based on opinions and suggestions from professionals and experts in the field relevant to the issue of ISSA. The relative weights for FA1 to FA6 are shown in Table-5 as follows:

Table5: Relative Weights for Focus-Areas

N	Focus-Areas	Weightings
1	(FA-1)The commitment to the ISS policy	30%
2	(FA-2)The effective use of passwords	20%
3	(FA-3)The safe usage of Internet and e-mail	15%
4	(FA-4)Being aware of ISS threats	15%
5	(FA-5)Backing up the important files	10%
6	(FA-6)The required updates for operating system and anti-virus program	10%

The overall evaluation value of ISSA requires a scale to describe the level of ISSA. A scale for ISSA in the current study has been developed according to Kruger and Kearney (2006) as shown in Table-6 as follows:

Table 6: Awareness Scale (Adapted from: Kruger and Kearney, 2006)

Level	scale	Actions required
Good	80% and more	No need for any new action.
Medium	From 60% to 79%	Attention is needed and some actions should be performed to improve to a better level.
Poor	Less than 60%	Actions are required and the required solutions have to be performed.

Data Analysis and Findings

This section presents the data analysis and the discussion of the study results in response to the research objectives, related to the evaluation of the level of Information Systems Security Awareness (ISSA) at KU. The section also includes a process of analyzing the variances to explore whether there are any significant differences in the results, between the study sample according to gender, age, qualification, and college.

Evaluation of Information Systems Security Awareness (ISSA) at KU

The process of evaluating ISSA at KU depends on analyzing questionnaire results related to the evaluation of the levels of three human awareness factors: knowledge, attitude and behavior regarding the following six ISS focus-areas (FA): (FA-1) Commitment to ISS policy, (FA-2) Effective use of passwords, (FA-3) Safe usage of Internet and e-mail, (FA-4) Being aware of ISS threats, (FA-5) Backing up the important files, (FA-6) Required updates for operating system and antivirus program. Each awareness factor is evaluated, and according to each FA using the responses to certain relevant questions in the questionnaire.

Evaluating Knowledge Factor

The evaluation of the knowledge factor is conducted in accordance with each of the six focus-areas (FA1 to FA6), using the relevant survey results. The levels of knowledge regarding the six focus-areas and the overall level at KU are illustrated in Figure-1.

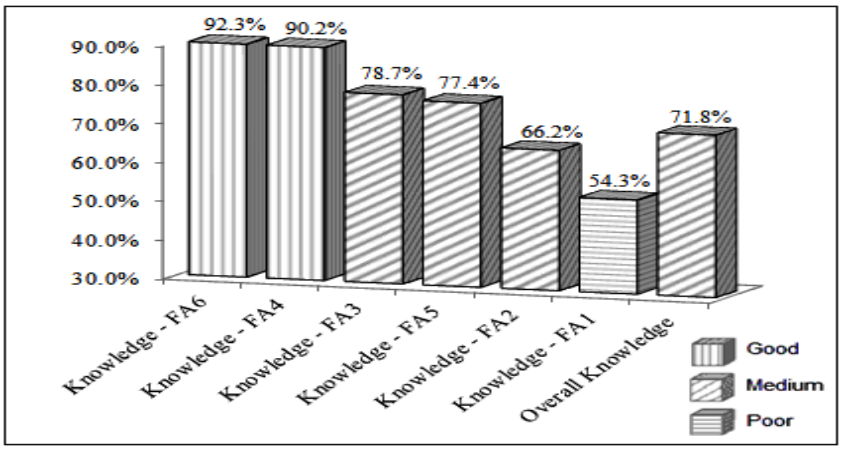

Figure1: Overall Knowledge Levels in Descending Order

It is shown from Figure-1 that the overall knowledge level of the end-users at KU colleges is medium, according to the awareness-scale (refer to Table-6).The results indicate that knowledge levels were more than 80%, i.e. good and no need for new actions, for the following focus-areas: required updates for operating system and antivirus program (FA-6), and being aware of ISS threats (FA-4). The results indicate that knowledge levels were equal to or more than 60% and less than 80%, i.e. medium, attention is needed and some actions should be performed to improve to a better level, for the following focus-areas: safe usage of Internet and e-mail (FA-3), backing up the important files (FA-5), and effective use of passwords (FA-2). Whereas, the results also indicate that the knowledge level was less than 60%, i.e. poor, actions are required and the solutions have to be performed, for the following focus-area: commitment to ISS policy (FA-1).

Evaluating Attitude Factor

The evaluation of the attitude factor is conducted in accordance with each of the six focus-areas (FA1 to FA6), using the relevant survey results. The levels of attitude regarding the six focus-areas and the overall level at KU are illustrated in Figure-2.

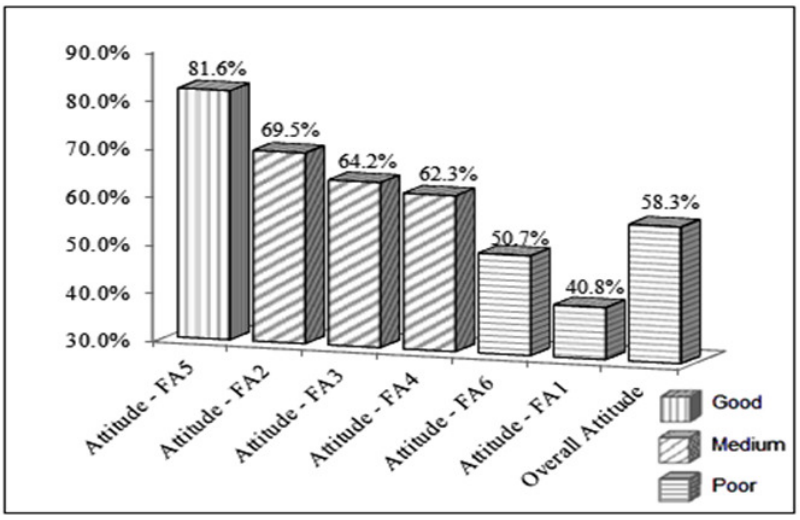

Figure 2: Overall Attitude Levels in Descending Order

It is shown from Figure-2 that the overall attitude level of the end-users at KU colleges is poor. Actions are required and solutions have to be performed. The results indicate that attitude levels were more than 80%, i.e. good and no need for new actions, for the following focus-area: backing up the important files (FA-5). The results also indicate that attitude levels were more than 60% and less than 80%, i.e. medium, attention is needed and some actions should be performed to improve to a better level, for the following focus-areas: effective use of passwords (FA-2), safe usage of Internet and e-mail (FA-3), and being aware of ISS threats (FA-4). Whereas, the results indicate that the attitude levels were less than 60%, i.e. poor, actions are required and the solutions have to be performed, for the focus-areas: required updates for operating system and antivirus program (FA-6), and commitment to ISS policy (FA-1).

Evaluating Behavior Factor

The evaluation of the behavior factor is conducted in accordance with each of the six focus-areas (FA1 to FA6), using the relevant survey results. The levels of behavior regarding the six focus-areas and The overall level at KU are illustrated in Figure-3.

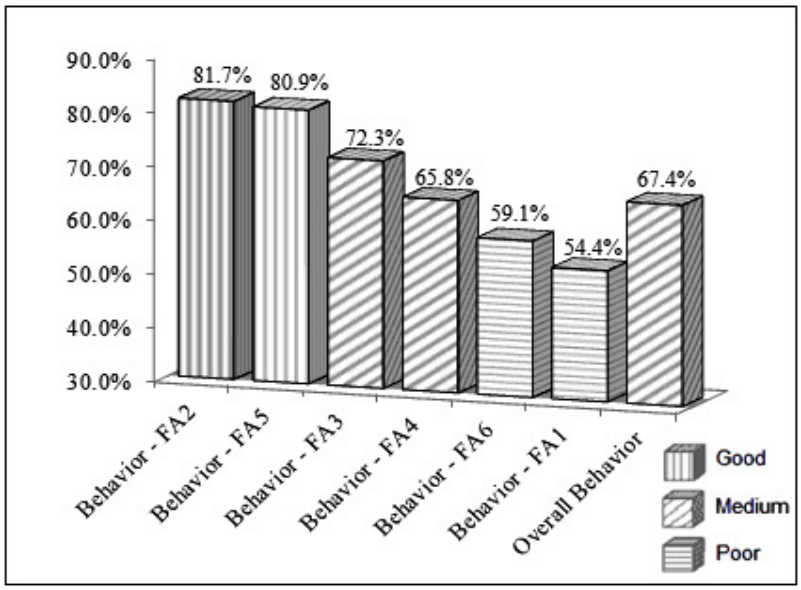

Figure 3: Overall Behavior Levels in Descending Order

According to Figure-3 and the awareness-scale, the overall behavior level of the end-users at KU colleges is medium. Attention is needed and some actions should be performed to improve ISSA to a better level. The results indicate that behavior levels were more than 80%, i.e. good, for the following focus-areas: backing up the important files (FA-5), and effective use of passwords (FA-2). The results also indicate that behavior levels were more than 60% and less than 80%, i.e. medium, for the following focus-areas: safe usage of Internet and e-mail (FA-3), and being aware of ISS threats (FA-4). Whereas, the results indicate that the behavior level was less than 60%, i.e. poor, for the following focus-areas: required updates for operating system and antivirus program (FA-6), and commitment to ISS policy (FA-1).

Overall Level of Information Systems Security Awareness (ISSA) at Kuwait University

The evaluation of the overall level of ISSA is based on the evaluation of the overall levels of knowledge, attitude and behavior. The overall level of ISSA is given, using the relative weights of awareness factors (knowledge, attitude and behavior), using formula (4-1). The overall levels of knowledge, attitude and behavior are 71.8%, 58.3% and 67.6% respectively, and their relative weights regarding the evaluation of ISSA are 0.3, 0.2 and 0.5 respectively, the overall ISSA level is calculated as follows:

Overall level of ISSA = (71.8% × 0.3) + (58.3% × 0.2) + (67.6% × 0.5) = 67%

According to awareness-scale, the overall level of ISSA is 67%, i.e. medium, attention is needed and some actions should be performed to improve to a better level. Table-7 summarizes the levels of knowledge, attitude, behavior and ISSA regarding the six focus-areas used in the study, and the relevant overall levels (weighted averages). The levels of ISSA regarding the six focus-areas used in the study are calculated using the previous formula for evaluating the overall level of ISSA, and the levels of knowledge, attitude and behavior regarding each one of the mentioned focus-areas.

Table7: Summary of Evaluation of ISSA at KU

Focus-Area	Awareness Factors			ISSA
	knowledge	Attitude	Behavior	
(FA-1): Commitment to ISS policy.	54.25%	40.8%	54.4%	51.7%
(FA-2): Effective use of passwords.	66.15%	69.5%	81.7%	74.6%
(FA-3): Safe usage of Internet and e-mail.	78.7%	64.2%	72.3%	72.6%
(FA-4): Being aware of ISS threats.	90.2%	62.3%	65.8%	72.4%
(FA-5): Backing up the important files.	77.4%	81.6%	83.4%	81.2%
(FA-6): Required updates for operating system and antivirus program.	92.3%	50.7%	59.10%	67.3%
Overall Level (Weighted Average)	71.8%	58.3%	67.6%	67 %

ISSA level varies according to the six focus-areas (FA-1 to FA-6). The results indicate that the end-users at KU have a good level of ISSA regarding backing up the important files (FA-5). The end-users at KU have medium levels of ISSA regarding effective use of passwords (FA-2), safe usage of Internet and e-mail (FA-3), being aware of ISS threats (FA-4), and required updates for operating system and antivirus program (FA-6). The end-users at KU have a poor level of ISSA regarding commitment to ISS policy (FA-1).

ISSA Levels at KU Colleges

The overall ISSA levels of KU colleges are illustrated in Figure-4, in descending order.

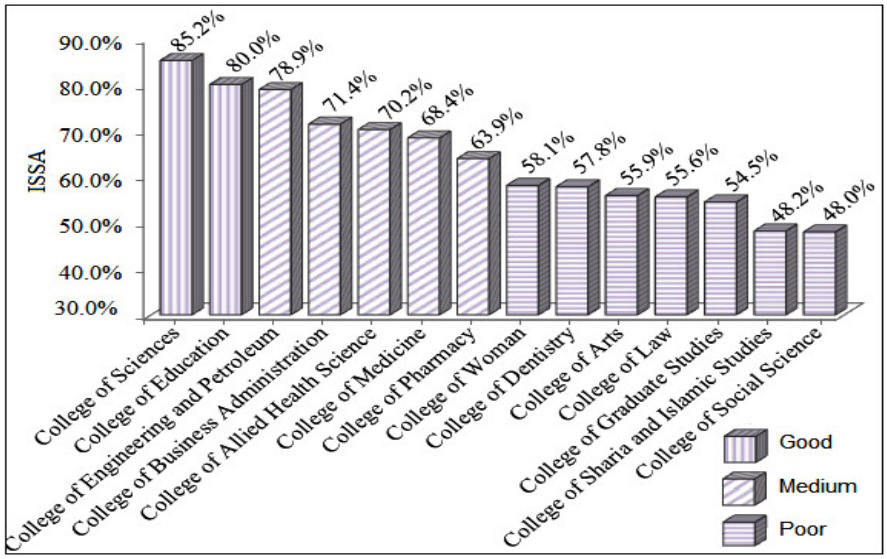

Figure 4: Overall ISSA Levels of KU Colleges in Descending Order

The results indicate that the overall ISSA level is more than 80%, i.e. good and no need for new actions, for only two colleges out of the fourteen colleges. These are: College of Sciences and College of Education, which have overall ISSA levels of 85.2% and 80% respectively. The results also indicate that the overall ISSA level is more than 60% and less than 80%, i.e. medium, attention is needed and some actions should be performed to improve to a better level, for five colleges out of the

fourteen colleges. These are: College of Engineering and Petroleum, College of Business Administration, College of Allied Health Science, College of Medicine, and College of Pharmacy, which have overall ISSA levels of 78.9%, 71.4%, 70.2%, 68.4%, and 63.9% respectively. Whereas, the results indicate that the overall ISSA level is less than 60%, i.e. poor, actions are required and the solutions have to be performed, for seven colleges out of the fourteen colleges. These are: College of Woman, College of Dentistry, College of Arts, College of Law, College of Graduate Studies, College of Sharia and Islamic Studies, and College of Social Science, which have overall ISSA levels of 58.1%, 57.8%, 55.9%, 55.6%, 54.5%, 48.2%, and 48% respectively. Table-8 summarizes these results.

Table 8: Overall ISSA levels at KU Colleges: Results Summary

Colleges	Number of Colleges	ISSA Level
College of Sciences – College of Education	2	Good
College of Engineering and Petroleum – College of Business Administration – College of Allied Health Science – College of Medicine – and College of Pharmacy	5	Medium
College of Woman – College of Dentistry – College of Arts, College of Law – College of Graduate Studies – College of Sharia and Islamic – Studies, and College of Social Science	7	Poor
Total Colleges = 14		

Conclusions and Recommendations

Based on the main objective of the study, the analysis and evaluation of Information Systems Security Awareness (ISSA) at KU, this section presents the study conclusions and the appropriate recommendations. Finally, the section presents some suggested future research.

Analysis and Breakdown of ISSA at KU

The level of ISSA at KU was evaluated by the summation of the overall levels of end-users' knowledge, attitude and behavior, after multiplying each one of them by its relative weight. The overall level of each one of knowledge, attitude and behavior was evaluated by the summation of its levels regarding ISS focus-areas, after multiplying each level by the relative weight of the relevant focus-area. The study showed that the ISS focus-areas regarding KU were six as follows: Commitment to ISS Policy (FA-1), Effective Use of Passwords (FA-2), Safe Usage of Internet and e-mail (FA-3), Being Aware of ISS Threats (FA-4), Backing up the Important Files (FA-5), and Required Updates for Operating System and Antivirus Program (FA-6). The breakdown of ISSA at KU is detailed in the next sub-sections, showing the overall levels of knowledge, attitude, behavior, and ISS, and their levels concerning each one of the six focus-areas.

Evaluating the Level of Knowledge

The study showed that the overall level of end-users' knowledge at KU was 71.8%. According to the awareness-scale, this level of knowledge is medium. The breakdown of the knowledge levels regarding the six ISS focus-areas showed that the knowledge levels were good regarding two of ISS focus-areas: FA-4 and FA-6, with 90.2% and 92.3% respectively. The good level indicates that no need for any new action. The knowledge levels were medium regarding three of ISS focus-areas: FA-2, FA-3, and FA-5, with 66.2%, 78.7%, and

77.4% respectively. The medium level indicates that attention is needed and some actions should be performed to improve to a better level. The knowledge level was poor regarding one of ISS focus-areas: FA-1, with 54.3%. The poor level indicates actions are required and relevant solutions have to be performed to raise the level.

Evaluating the Level of Attitude

The study showed that the overall level of end-users' attitude at KU was 58.3%. According to the awareness-scale, this level of attitude is poor. The breakdown of the attitude levels regarding the six ISS focus-areas showed that the attitude level was good regarding one of ISS focus-areas: FA-5, with 81.6%. The attitude levels were medium regarding three of ISS focus-areas: FA-2, FA-3, FA-4, with 69.5%, 64.2%, and 62.3% respectively. The attitude levels were poor regarding two of ISS focus-areas: FA-1 and FA-6, with 40.8% and 59.7% respectively.

Evaluating the level of Behavior

The study showed that the overall level of end-users' behavior at KU was 67.4%. According to the awareness-scale, this level of behavior is medium. The breakdown of the behavior levels regarding the six ISS focus-areas showed that the behavior levels were good regarding two of ISS focus-areas: FA-2, and FA-5, with 81.7% and 80.9% respectively. The behavior levels were medium regarding two of ISS focus-areas: FA-3, FA-4, with 72.3% and 65.8% respectively. The behavior levels were poor regarding two of ISS focus-areas: FA-1 and FA-6, with 54.4 and 59.1% respectively.

Evaluating the Level of ISSA at KU

The overall level of ISSA at KU was 67%. According to the awareness-scale, this level of ISSA is medium. The breakdown of ISSA levels regarding the six ISS focus-areas showed that the level of ISSA was good regarding one of ISS focus-areas: FA-5, with 81.2%. The levels of ISSA were medium regarding four of ISS focus-areas FA-2, FA-3, FA-4, and FA-6, with 74.6%, 72.6%, 72.4%, and 67.3% respectively. The levels of ISSA were poor regarding one of ISS focus-areas: FA-1, with 51.7%.

The Levels of ISSA at KU Colleges

The breakdown of the overall ISSA level regarding each of the fourteen KU colleges showed that the overall levels of ISSA were good regarding two colleges: College of Sciences and College of Education, with 85.2% and 80% respectively. The levels of ISSA were medium regarding five colleges: College of Engineering and Petroleum, College of Business Administration, College of Allied Health Science, College of Medicine, and College of Pharmacy, with 78.9%, 71.4%, 70.2%, 68.4%, and 63.9% respectively. The levels of ISSA were poor regarding seven colleges: College of Woman, College of Dentistry, College of Arts, College of Law, College of Graduate Studies, College of Sharia and Islamic, Studies, College of Social Science, with 58.1%, 57.8%, 55.9%, 55.6%, 54.5%, 48.2%, and 48% respectively.

Recommendations to Improve ISSA at KU

Based on the study results, the following recommendations are suggested to improve the overall level of ISSA at KU:

- *Recommendation to improve the Level of Attitude at KU:* Since the overall attitude level at KU was poor, it is highly recommended to find and apply the appropriate solutions to raise the overall attitude level. Priority should be given to the process of raising the overall attitude level, and should concentrate on the focus-areas: FA-1 and FA-6, as the relevant attitude levels in these areas were poor.

- *Recommendation to improve the Level of Knowledge at KU:* Since the overall knowledge level at KU was medium, it is recommended to provide some solutions to improve the overall knowledge to a better level. Priority for improving the overall knowledge level should concentrate on the focus-areas: FA-1, as the relevant knowledge level in this area was evaluated as poor.

- *Recommendation to improve the Level of Behavior at KU:* Since the overall behavior level at KU was medium, it is recommended to provide some solutions to improve the overall behavior to a better level. Priority of improving the overall behavior level should concentrate on the focus-areas: FA-1, and FA-6, as the relevant behavior levels in these areas were poor.

- *Recommendation Regarding KU Colleges:* The study results showed seven colleges with poor overall levels of ISSA, these are: College of Woman, College of Dentistry, College of Arts, College of Law, College of Graduate Studies, College of Sharia and Islamic Studies, and College of Social Science. It is recommended for the process of improving the overall level at KU to give priority to these mentioned colleges when planning the appropriate solutions to raise the overall level of ISSA at KU.

- *General Recommendations:* The general recommendations for this study are to

a) Carry out awareness campaigns in the university to educate employees about the importance of ISSA issue;
b) Evaluate the level of ISSA of the employees periodically to ensure the adequate level, or stand on any shortcomings to set the appropriate solutions such as the training program.

Suggestions for Future Research

This study is related to ISSA of the end-users and limited to the sample unit pertaining to KU. However, the study procedures can be applied for the other universities and some similar institutions. The procedures include identifying the human awareness factors and generating ISS focus-areas according to the targeted organization, to be used in calculating the overall level of ISSA of the end-users. Suggested research can be conducted on the following:

a) Organizational culture and the issue of information systems security awareness in the institutions.
b) Comparison study between the public sector and the private sector in countries of the Gulf Cooperation Council (GCC) regarding the issue of information systems security awareness.
c) Comparison study between the universities of developed countries and developing countries regarding the issue of information systems security awareness.
d) Ethics regarding the issue of information systems security.

References

1. Ajzen, I., (1991). 'The theory of planned behavior'. Journal of Organizational Behavior and Human Decision Processes, 50(2), pp. 179 - 211.

2. Al-Alawi, A. I. (2014), 'Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status', Research Journal of Business Management, 8(3), pp139-156,
DOI: 10.3923/rjbm.2014.139.156

3. Al-Alawi, A.I (2011), E-strategies for Resource Management Systems Planning and Implementation, edited by Eshaa M. Alkhlifa, Business Science Reference as imprint of IGI Global, Hershey, NY

4. Al-Alawi, A. I. & Hafedh, E. A., (2006). 'Auditing of Information Privacy'. Journal of Information Technology, 5(1), pp. 177-182.

5. Al-Alawi, A.I. and Al-Amer, M.A, (2006) 'Young Generation Attitudes and Awareness Towards the Implementation of Smart Card in Bahrain: An Exploratory Study', Journal of Computer Science; DOI: 10.3844/jcssp.2006.441.446 Source: DOAJ

6. Albrechtsen, E. & Hovden, J., (2010). 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study'. Journal of Computer and Security, 29(2010),pp. 432 – 445.

7. Brooks, W. M., Warner, M. J. & Hutchinson, W., 2002. 'A Security Evaluation Crieria'. Journal of Logistics Information Management, 15((5/6)), pp. 377 – 384

8. CNSS (2015), Committee on National Security Systems, CNSSI No. 1300, [online], [Retrieved June 22, 2014], https://www.cnss.gov/cnss

9. Cochran, W. G., (1977). Sampling techniques. Third ed. New York: John Wiley & Sons.

10.Cornell University Law School (2015), Legal Information Institute, 44 U.S. Code § 3542 – Definitions, [online] [Retrieved 12 June 2015] https://www.law.cornell.edu/uscode/text/44/3542,

11.Dlamini, M. T., Eloff, J. H. & Eloff, M. M., (2009). 'Information security: The moving target'. Journal of Computers and Security, 28(3/4), pp. 189-198.

12.Drevin, L., Kruger, H. A. & Steyn, T., (2007). 'Value - focused assessment of ICT security awareness in an academic environment'. Journal of Computer and Security, 26(1), pp. 36 - 43.

13.Fabrigar, L. R., .Petty, R. E., Smith, S. M. & Crites, S. L., (2006). 'Understanding knowledge effects on attitude–behavior consistency: The role of relevance, complexity, and amount of knowledge'. Journal of Personal Social Psychology, 90(4), pp. 556 - 577.

14.Feldman, R. S., (1999). Understanding Psychology. 5th edition ed. Boston: River Ridge, IL..

15.Feng, N. & Li, M., (2011). 'An information systems security risk assessment model under uncertain environment'. Journal of Applied Soft Computing, 11(7), pp. 4332-4340.

16.Furnell, S. M. et al., (1996). 'Assessing staff attitudes towards information security in a European healthcare establishment'. Journal of Medical Informatics, 21(2), pp. 105-112.

17.Hansche, S., (2001). 'Designing a security awareness program: part I'. Journal of Information System Security, 10(1), pp. 14–22..

18.Humphreys, E. J., Moses, R. H. & Plate, A. E., (1998). Risk Assessment and Risk Management. London: BSI.

19.Hwang, Y., Kim, S. & Jeng, J., (2000). 'Examining the causal relationships among selected antecedents of responsible environmental behavior'. Journal of Environmental and Education, 31(4), pp. 19 - 25.

20.Information Security Forum (ISF), (2003). The standard of good practice for information security. [Online], [Retrieved 14th March 2011]. https://www.securityforumrg/

21.ISACA (2015), Information Systems Audit and Control Association, CISM Review Manual, [online] [Retrieved 12th June 2015], http://www.isaca.org/bookstore/extras/Pages/English-CISM-Review-Manual-2015.aspx

22.Israel, G. D., (1992). Determining Sample Size. [Online], [Retrieved 13th September 2013]. : http://edis.ifas.ufl.edu/pd006

23.Gerber, M. & Solms, R. V., (2001). 'From risk analysis to security requirements'. Journal of Computer and Security, 20(7), pp. 577-584.

24.Gopi, M. & Ramayah, T., (2007). 'Applicability of theory of planned behavior in predicting intention to trade online: Some evidence from a developing country'. Journal of International Emerging Markets, 2(4), pp. 348-360.

25.Kallgren, C. A. & Wood, W., (1986). 'Access to attitude - relevant information in memory as a determinant of attitude - behavior consistency'. Journal of Experimental Social Psychology, 22(1), pp. 328 - 338.

26.Kankanhalli, A., Teo, H. -. H., Tan, B. C. & Wei, K. -. K., 2003. 'An integrative study of information systems security effectiveness'. Journal of Information Management, 23(1), pp. 139 - 154.

27.Karat, J. & Karat, C. M., (2003). 'The evolution of user-centered focus in the human computer interaction field'. Journal of IBM Systems, 42(4), pp. 532–541.

28.Karyda, M., Kiountouzis, E. & Kokolakis, S., (2005). 'Information systems security policies: a contextual perspective'. Journal of Computer and Security , 24(1), pp. 246 - 260.

29.Keeney, R. L., (1994). 'Creativity in Decision Making with Value - Focused Thinking'. Journal of Sloan Management Review, 35(4), pp. 33 - 41.

30.Kruger, H. A. & Kearney, W. D., (2006). 'A prototype for assessing information security awareness'. Journal of Computer and Security, 25(1), pp. 289 - 296.

31.Kuwait University (KU), (2010). About KU. [Online], [Retrieved 5th January 2011] : http://www.kuniv.edu/ku

32.Lichtenberg, E. & Zimmerman, R., (1999). 'Adverse Health Effects, Environmental Attitudes, and Pesticide Usage Behavior of Farm Operators'. Journal of Risk Analysis - An International Journal, 19(2), pp. 283 - 294.

33.Martha, A., Iain, W. & Ngaire, ,. D., (2006). Social Cognition: An Integrated Approach. Second Ed. London: SAGE Publisher.

34.NIST, (2004), National Institute of Standards and Technology. Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg (MD): NIST: FIPS PUB 199.

35.Offor, P.I. & Gurvirender, T (2014), 'Information Systems Security Training in Organizations: Andragogical Perspective', Information Systems Security, Assurance, and Privacy Track (SIGSEC), 20th Americas Conference on Information Systems, August 9, 2014, Savannah, Georgia, USA

36.Oxford Dictionaries, (2014). Dictionary. [Online]. [Retrieved 5th September 2014]. http://www.oxforddictionaries.com,

37.Pahnila, S., Siponen, M. & Mahmood, A., (2007). Employees' Behavior towards IS Security Policy Compliance.. Hawaii, IEEE Computer Society.

38.Posthumus, S. & Solms, R. V., (2004). 'A framework for the governance of information security'. Journal of Computer and Security, 23(1), pp. 638-646.

39.Rezgui, Y. & Marks, A., (2008). 'Information security awareness in higher education: An exploratory study'. Journal of Computer and Security , 27(1), pp. 241 - 253.

40.Rezmierski, V. E., Seese, M. R. & Clair II, N. S., (2002). 'University systems security logging: who is doing it and how far can they go?'. Journal of Computer and Security, 21(6), pp. 557 - 564.

41.Ritchie, B. & Brindley, C., (2001). 'The information-risk conundrum'. Journal of Marketing Intelligence and Planning, 19(1), pp. 29-37.

42.Ross, S. T., 1999. UNIX System Security Tools. McGraw-Hill: ISBN: 0-079-13788-1.

43.Rogers, R. W. & Prentice - Dunn, S., (1997). Protection motivation theory. In D. S. Gochman (Ed.), Handbook of Health Behavior Research I: Personal and Social Determinants. New York: NY: Plenum Press.

44.Ryan, J. J. & Ryan, D. J., (2006). 'Expected benefits of information security investments'. Journal of computers and security, 25(1), pp. 579-588.

45.Singh, A.N, Picot, A., Kranz, J, Gupta, M.P, Ojha, A. (2013), 'Information security management (ism) practices: Lessons from select cases from India and Germany', Global Journal of Flexible Systems Management, 14(4), pp. 225-239

46.Sirma, J,, Muiru, M. and Kipchillat, C. (2014), 'Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities',

Information and Knowledge Management, 4(9), ISSN 2224-5758

47.Siponen, M. T., (2005). 'Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods'. Journal of Information and Organization, 15(1), pp. 339 - 375.

48.Solms, R. V., (1996). 'Information Security Management: The Second Generation'. Journal of Computer and security, 15(1), pp. 281-288.

49.Stoneburner, G., Goguen, A. & Feringa, A., (2002). Risk Management Guide for Information Technology Systems, s.l.: s.n.

50.Thellufsen, C., Abbas Rajabifard, A. R., Enemark, S. & Williamson, I., (2009). 'Awareness as a foundation for developing effective spatial data infrastructures'. Journal of Land Use Policy, 26(1), pp. 254-261.

51.Tipton, H.F. & Krause, M. (2007), Information Security Management Handbook, 6th ed., Auerbach Publications, Tylor & Francis Group

52.Thomson, K.-L. & Solms, R. V., (2005). 'Information security obedience: a definition'. Journal of Computer and Security, 24(1), pp. 69-75.

53.Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E., (2005). 'The insider threat to information systems and the effectiveness of ISO1779'. Journal of Computer and Security, 24(1), pp. 472 - 484.

54.Turban, E., Volonino, L., and Wood, G.R,. (2015), Information technology for management: digital strategies for insight, action, and sustainable performance, 10th ed: Hoboken, NJ: Wiley

55.Updegrove, D. & Wishon, G., (2003). Computers and Network Security in Higher Education, San Francisco: Jossey-Bass Inc .

56.Veiga, A. D. & Eloff, J. H., (2010). 'A framework and assessment instrument for information security culture'. Journal of Computer and Security, 29(1), pp. 196 - 207.

57.Watson, R. T., (2007). Information Systems. Zurich, Switzerland: Global Text Project.

58.Whitman, M. E., Mattord, H. J. & Mattord, H. J., 2004. Principles of information security. Second ed. Independence, KY: Course Technology.

59.Williams, P. & Andersen, (2001). 'Information Security Governance'. Journal of Information Security Technical Report, 6(3), pp. 60-70.

60.Wilson, M. & Hash, J., (2003). Building an Information Technology Security Awareness and Training Program, s.l.: s.n.

61.Woon, I. M. Y., Tan, G. W. & Low, R. T., (2005). A protection motivation theory approach to home wireless security. Las Vegas, s.n., pp. 367-380.

62.Zissis, D. & Lekkas, D., (2010). 'Addressing cloud computing security issues'. Journal of Future Generation Computer Systems, 28(2012), pp. 583-592.