ISSN:0975-9646

Critical Evaluation of the Challenges Associated With Information System Security Awareness

Mansoor Ahmed Alshehi
PhD Candidate
School of Computing, Creative Technologies & Engineering
Leeds Beckett University, UK

Dr. Muthu Ramachandran
Principal Lecturer
School of Computing, Creative Technologies & Engineering
Leeds Beckett University

Dr. Hissam Tawfik
Professor
School of Computing, Creative Technologies & Engineering
Leeds Beckett University

Abstract: Information system (IS) security is fundamental to protect the confidential data from unwanted threats. Similarly, with respect to security agencies in public sector, the protection IS assets is important from both internal and external security. Mostly, it is found that organizations widely focus on external security while overlooked the internal security measures mainly associated with the human resource i.e. behaviour of IS users toward security. Therefore, this study specifically focuses on the awareness of human resource since employees in an organization must be aware of the significance of the systems' protection as they play fundamental role in securing or destroying IS of an organization. This study sheds light on the awareness among the employees in the UAE law enforcement agencies since they are responsible for the protection of homeland as well as the public data and information due to which the high level of security have to be ensured. The methodology adopted to achieve the study purpose is based on the quantitative method in which survey was conducted from randomly selected 500 employees working in the UAE law enforcement agencies. The results revealed that the awareness and behaviour competencies of IS users about security controls develop a greater sense of protecting and securing the potential information assets of an organization, but in the UAE law enforcement agencies, the unsatisfactory level of awareness has been identified. In result, Information System Security Awareness and Behaviour Competence Model (ISSABCM) is developed and suggested for the UAE law enforcement agencies that matches with their culture as well as fill the gaps in existing awareness models.

I. INTRODUCTION

The significance of information system security cannot be over-estimated in present networked corporate world. By integrating a potent security awareness program, the organizations can reduce the risks of security breach in the information assets (Puhakainen, & Siponen, 2010). One of the major issues faced by the enterprises in context to information system security is the lack of significance given to an implementation program of security awareness in their facilities. If the firms or employees are unaware of this fact, then, they place the firm's privileged evidence at high risk while committing security breaches (Kritzinger, & von Solms, 2010). Henceforth, a potential and competent information security program is successfully implemented by implementing an awareness and training program for the employees while addressing the procedures, policies and tools. Their learning should consist of awareness to remind the employees what is expected, training to teach a skill to use the required tool and education to support the required tool to be used securely in a firm (Ahmad, Maynard, & Park, 2014). Insufficient security and safety measure programs may lead to various types of vulnerabilities like theft of data or loss of information.

Similarly, in public sector, especially among the law enforcement agencies responsible for the security of public data and homeland as whole, the role of IS cannot be neglected. The changing global technology trend whereas allowed those agencies to execute their operations in efficient manner, on the other hand, it has created a greater challenge for them in terms of protection and secure use of certain systems. It is reported in many studies that law enforcement agencies are remain at risk due to security breaches, data leakage, hacking and so on (Rose, 2000; Andreas, 2003; Chen at al., 2004; Richardson and Director, 2008, Crossler, et al., 2013). Similarly, literature also supported that these security risks in law enforcement agencies mainly occur due to human factor i.e. irresponsible behaviour of employees or IS users (Crowley, 2003; D'Arcy et al., 2009; Herath and Rao, 2009; Ifinedo, 2012). It implies that in law enforcement agencies, the security should be at first priority; therefore, along with various internal and external security measures such as strong passwords, security policies, international standards, and antiviruses, the equal importance should be given toward the awareness and positive behaviour of employees or IS users in certain organization. It is supported by Bulgurcu et al. (2010) that only well-informed and responsive employees play fundamental role in making security measures successful as well as ensure the best level of security by considering it as prime responsibility.

Global law enforcement agencies have confirmed the importance and prominence of employees' awareness toward information system security (ISS) by introducing and implementing different ISS awareness programs and approaches. An example can be taken from the Missouri Police Department that has introduced the security awareness training program for the employees working in the department at different level to develop their awareness related to ISS protection (Missouri Police, 2012). Similarly, 'CJIS Online' awareness training software was also introduced by Criminal Justice Information Service (CJIS) for the law enforcement agencies in Texas, USA to provide training to employees concerning to different security measures (CJIS, 2016). Thus, it can be said that employees' awareness in law enforcement agencies is fundamental due to which governments and the agencies themselves are making efforts towards integrating ISS awareness approach. ISS is also perceived as a tool of fighting and avoiding criminal activities like malware, virus and hacking which constitute issues. Concerning to the mentioned facts, this study sheds light on the awareness among the employees in the UAE law enforcement agencies since they are responsible for the protection of homeland as well as the public data and information due to which the high level of security have to be ensured. For this purpose, awareness level among the employees is identified and various ISS awareness approaches are critically evaluated to find the best solution for the UAE law enforcement agencies. Thus, the following research has been conducted to understand-

What are the challenges associated with information system security in an organization? Why is it necessary to implement information system security awareness program in a firm?

II. LITERATURE REVIEW

Information System (IS), often referred to a system, is used to produce, obtain, save or process the electrical information or data. It is also known as a mechanism of various components including software and hardware, proficient workers and infrastructure that is used to plan, coordinate, finalization of decisions and transformation of data inside or outside the association. It offers great help for the data intensive applications that are meant to process huge size of data with the use of parallel approach (Poepjes & Lane, 2012). In recent times, IS is available at personal level to perform daily routine tasks and at organizational level to complete complex business processes (Myers & Klein, 2011; Case, 2012). Moreover, to increase the effectiveness of public services delivery and to preserve the public records in cost operational and well-organized way IS offers great help to the government organizations (Cordella & Iannacci, 2010). Considering this, it can be said that information systems are highly operative in both public and private institutes.

However, with the excessive use of IS around the globe, an important issue of security and safety of the IS has now emerged significantly. This is due to the fact that the large amount of data is transformed from one place to another that can be result into data seepage and information revelation in case of improper control and inefficient security regarding information protection (Whitman & Mattord, 2010). In the given case, IS security refers to the safety of the system that is meant to sort the information and data. To safeguard such security, various tools can be used including software and physical protection such as securing system inside a specific location or restriction over the system access (Bainbridge, 2011).

The execution of operative security system enables to lower the harmful consequences of data seepage (Whitman & Mattord, 2010). The security of IS must be designed in way to ensure the confidentiality, consistency and availability of the data. Whiteman and Mattord (2010) explored that the need to have an effective ISS emerged during late nineteen's as a result of great disruptions in various computers were generated by multiple damaging viruses including Melissa and Red Code etc. From that time to now, numerous viruses had been developed designed to damage the security of IS and to exert harmful effect over the overall performance of the system.

Additionally, Poepjes and Lane (2012) found that the risk towards ISS intensified during 2012 when the email threats were arrived. Later, the arrival of mobile phone threats caused the death of many individuals who were not ready to pay the attractive amount of ransom. Such security threats came in the form of numbers like the phishing emails, designed to ask the corporation of the consumers regarding their bank account numbers and passwords to snatch their money. The illustration of such threats can be found in Nigerian Scam that had been recorded by Securities and Investments Commission of Australia. Moreover, during 2007, Institute of Computer Security exposed that the ineffective ISS caused many financial loss (the estimate average were $168,000 to $350,424) leading to the unsuccessful system protection and virus attacks (Poepjes & Lane, 2012).

It has also been found that around 70% of extortions to ISS of any institutes pledges from the inner factors (Sanyal et al., 2010). These internal factors includes existing or former workers, business associates, suppliers and other persons who possess the easy access of organization's networks and servers (Sanyal et al., 2010). Many studies have found that most important internal factor is the given case is employee of any organizations as they can have easy and great access to the IS and so they can easily leak the data and information. For instance, Access Governance Trends had conducted a research in which more than 80% of the respondents responded that the internal workers of the organizations who have great access to the system cause data and information seepage (Ponemon Institute, 2010). Similar results were found by another study conducted by Corona (2010). The study found that organization's employee can leak information due to many reasons including strangeness of the IS process, not obeying the recognized ISS procedures and ineffective execution of the information regarding the assigned assignments (Corona, 2010).

The empirical research provide evidence that the protection of IS from any kind of threat is linked with the understanding of the users and employees about ISS (Sanyal, et al., 2010; Whitman & Mattord, 2010; Corona,

2010; Ponemon Institute, 2010; Poepjes & Lane, 2012). According to Poepjes & Lane (2012), in current working age, the employees should have well understanding about their role in protecting the IS. Similarly another study mentioned that employees are being involved in the risky behaviour because they can easily open any attachments on the internet that affect the proprietary information, can cause threats to the corporate networks. Along with this, the employees do not consider security threats in their routine life that create risk for the IS of the company (Nicolaisen, 2010). If the employee properly maintain and implement the IS security, then it could become the competitive advantage for the company. So, it can be stated that Lack of awareness for the ISS is an important reason for that create threats and complexities to the IS security.

III. ISS AWARENESS MODELS, THEORIES AND APPROACHES

Since, the lack of awareness for ISS has been evolved rapidly but the researchers and practitioners consistently finding out how to resolve the problems caused by lack of awareness. The literature shows that understanding about ISS can be enhanced by training programs. It can also be done using awareness campaigns or education scheme or providing them with the security related information (Bulgurcu, et al., 2010; Corona, 2010; Lebek, et al., 2013; Albrechtsen & Hovden, 2010). Precisely, it is stated that the concept of awareness of ISS consist of three prime elements. These elements include education, training and attentiveness, that enable the users to operate IS in safe and secure manner.

Besides providing adequate evidence regarding the ISS awareness models, theories and approaches, it is important to understand the concept of Information System Security Awareness programs and the reasons for implementing it in a firm.

ISSA (Information System Security Awareness) program-

According to D'Arcy, Hovav, & Galletta (2009), the development of an information safety security policy, standard, procedure and guideline is the beginning of a compelling information system security program. Most of the organizations face issues of improper implementation of information system security awareness programs which might result into high risks of security breaches. The information system security protocol is effective with the implementation of the information system security awareness or ISSA program (Stallings, Brown, Bauer, & Bhattacharjee, 2012). This helps in providing proper training to the employees and help them to see the policies, processes or tools followed in the organization to avoid challenges or cyber threats. By creating awareness programs, Shaw, Chen, Harris, & Huang (2009) noted that the firm can communicate the important information to the staffs which requires further learning, understanding, required skills and obtaining enough knowledge. This would also result into a success of the awareness program. It is also said that the success of security awareness program is dependent on the changes in an individual behaviour. Laptop theft, unauthorized access, insider abuse and viruses are the common incidents that are faced by the firms if they are not aware of the information system security awareness program. Puhakainen, & Siponen (2010) noted that if individual disregards the security policy or procedure, then, the company is left at risks. The information system security awareness program needs to be updated with innovative methods by notifying the people who prefer to obtain the company information through non-technical (social engineering) and technical (spyware) methods.

Training and security awareness are the important components of the information system security programs. the training and awareness program for the employees plays a significant role in providing holistic information security goals and meet its total security solutions. argued that this is only possible if the overall workforce participates in the program. Henceforth, the company needs to train its workforce continually based on the security responsibilities and policies so that it can experience high success rate in terms of protecting the information assets of the firm. Thus, the workforce is the significant factor in maintaining security instead of the technology (Kritzinger, & von Solms, 2010). Depending on this, the researcher has provided further information on the basis of information system security awareness program model, the policies and procedures associated with it and the need of training programs.

In literature, there are numbers of theories and models of IS security awareness have been proposed by different authors that explain the way through which awareness among employees can be improved; these are:

A. Information Security Awareness Capability Model

ISACM (Information Security Awareness Capability Model) was introduced by Poepjes and Lane in 2012 to identify the awareness gaps and associated risks to IS security controls of an organization (Poepjes & Lane, 2012). The model has 3 key components that include Awareness Importance, Awareness Capability, and Awareness Risk, which determines the importance of awareness and its influence on the performance of an IS process or control; examines capability of a person regarding making decision; and highlights gap obtained from the required amount of awareness being larger than that really being shown respectively. The reliability aspects of ISACM are that these three components are based on the controls given within the ISO (International Standard Organization) 27002 (Poepjes & Lane, 2012). However, the integration of ISO 27002 whereas identified effective for the ISSA, but a limitation of the ISO 27002 is that it is not applicable for every organization because of different nature of every organization and their approaches to manage IS security. This gap is left by the researcher and need to be filled by finding out a new model, which could also be implemented in every organization regardless of their business nature (Poepjes & Lane, 2012).

B. Policies and Standards Development

The goal and objective of an enterprise is to protect its assets by implementing several policies, procedures and standards as per the need. Bulgurcu, Cavusoglu, & Benbasat (2010) stated that the policies are introduced to the employees to make them aware regarding how to

handle the assets so that it may not lead to any mishaps like theft of system or loss of data. There are numbers of IS security and awareness policies and standards have been developed and implemented throughout the world. For instance, BSI (Bundesamt für Sicherheit in der Informationstechnik) in English known as the Federal Office for Information Security, is responsible for managing IT security for the German Government. This standard is completely compatible with ISO standard 27001 and 2700x. BSI standard 100-1 to 100-4 ensures the protection of IS and information at higher level, but has one limitation too since, this approach only works successfully with IT-Grundschutz. Warkentin, & Willison (2009) noted that if an organization does not follow the BSI standard 100-2, it would not able to implement the BSI standard 100-3 (Federal Office for Information Security, 2014). It means that BSI standard does not work solely without the support of IT-Grundschutz and thus, it is considerable weakness of this approach.

Another example is Data Protection Act Principle 7: Information Security, a British Act of Parliament, which provide protection and security to the organisational data and IS assets from administrative, physical, and technical perspectives (Information Commissioner's Office, 2014). Whereas the principle is full of guidelines and laws regarding to protect the information and IS, on the other hand, the law is very difficult and full of complexities (Bainbridge, 2011). According to Birkinshaw (2010) the interpretation of the act is not simple since numbers of organisations seem unsure about the purpose of this principle. Additionaly, it does not provide the basic information that have to be avilable publicly by restricting it (Parliament & Committee, 2012). Besides, it also influences the way through which organisations perform business operations.

Another common standard that is practicing throughout the world is ISO standards. There are several ISO Standards working efficiently, but have these standards have some limitations too. For instance, ISO 13335:2004 provides formal guidelines about the management and implementation of IT (information technology) security and management process. The limitation of this standard is that it provides instructions only since no solutions are given regarding the management of IT or IS security (Kouns & Minoli, 2011). Similarly, ISO 27001:2013 is a relatively new standard, which provides detailed recommendations on the introduction, operation, risk and perfection of an information security management system, but it does not provide sufficient assistance for the practical implementation of such security measure (Calder, 2012). The next widely acceptable ISO standard is ISO 27002:2013, a reorganization of ISO 17799:2005, which determines a framework for information security management incorporating guidelines about the steps require to develop well-working security management system to secure an organisation. Besides, it also include the recommendations to the organizations to protect IS, but has no technical information given for the protection of information (ISO Directory, 2014). Hence, it is depicted that these ISO standards widely contribute to improving the understanding, practical implication process, measurability of risks, and risk management, but there are no single standards, which can be fully implemented to support the IS security (Kang, 2013). These are the easiest security processes included in policies which are measured to justif the return on investments. Step by step proceses are used to finish a task. the procedures provide the users with an information which is needed to complete a proper task while ensuring the organization that the tasks are finished in an approved and uniform manner. The procedures enhance the efficiencies in the employee workflow while assisting the prevention of the fraud and misues. Standards ensure that the systems and the programs are working together. Further, Knapp, Morris Jr, Marshall, & Byrd (2009) added that it also helps in error searching through the old code which is better in undertsanding the issues. Bulgurcu, Cavusoglu, & Benbasat (2010) noted that by developing the standards, an enterprise limits the rough applications, platforms, systems, hardware or software. Standards are also cost-saving processes which support the successful running of an enterprise.

C. Awareness Training Programs

The initiation of awareness training program is another way through which the awareness can be increased among IS users to use system protectively. Puhakainen and Siponen (2010) argued that training is an essential part of an organisation which plays significant role in protecting the IS by informing employees about IS security related policies & standards and making them responsive toward the risks associated with improper use of IS (Puhakainen & Siponen, 2010).

Different researchers determined different training and awareness programs for IS protection and security. For instance, Karjalainen and Siponen (2011) presented a prototype tool for the training related to increase the awareness about ISS, which allow employee to learn through self-packed security training, in which they are provided with an effective environment that permits the learners to simulate the security measures for the numbers of pre-defined case study examples. This training approach is effective in terms of increasing familiarity of employees about the available kinds of countermeasures, circumstances in which they feels comfortable and any restraints that they have to oblige. Besides, the authors stated that this training approach is mainly useful in small organisations which have lacking of professional knowledge and ISS related concerns require to be addressed by the workforce (Karjalainen & Siponen, 2011).

According to Puhakainen, & Siponen, (2010), there is a need of developing individual responsibilities to maintain and control the system and save it from threats or other system related risks. It has been noted in some cases that whenever there is a breakdown of system or virus attack, the individuals become unsuccessful in resolving the issue and make the system virus free. If the employees have a negative attitude and the security breaches in the firms, then, it might become a IT security threat. Henceforth, Karjalainen, & Siponen (2011) suggested that the staffs need proper training and education regarding the

information system security awareness programs so that they can take their individual responsibilities and secure the systems and firms from external and internal threats. Besides individual responsibilities, the employee capability is another important factor which needs to be improved through training and education on the basis of security awareness of information system. In this respect, Aloul (2012) commented that in certain cases, if there are system breakdowns or virus attacks in the systems, then, the IT staffs become incapable of solving it. They need the help of IT experts or seniors to fix the issue. This is because they do not have any awareness knowledge of the information system security operated by them. Puhakainen, & Siponen (2010) added that these employees lack in terms of receiving proper training in their firms. Henceforth, they need appropriate training to resolve such issues and gather enough knowledge on the same. This will also help them to get some idea regarding preventive measures used in avoiding the threats related to the system. Proper training and programs enhance the ethical behaviour of the workforce while making them aware of the method of using the tools and fixing the system so that the virus can be avoided (D'Arcy, Hovav, & Galletta, 2009). The workforce will also develop a secured behaviour where they will manage and control all the risks which might rise from the system.

He and Johnson (2012) conducted a research in a healthcare organisation, in which they argued that ISS could not be promoted without the implementation and utilization of ISS awareness training. However, He and Johnson (2012) suggested that the training program must cover key areas of ISS i.e. analysis of day-to-day responsibilities of IS users; training for the secure use of IS; training to deal with particular issues like new viruses attack on system; proper employees segmentation during training; and define clear roles of establishing, implementing and delivering training program (He & Johnson, 2012). Similarly, Knapp & Ferrante (2012), presented another example of an ISSA program, which consisted of two parts, i.e. Awareness Briefings contains training sessions, and Continuing Awareness Material contains printed stuff (Knapp & Ferrante, 2012). It highlights that the training program should be delivered through briefings such as training sessions and continuing awareness stuff such as printed material (posters or booklets) (Herold, 2010). Lehrfeld, et al., (2013) claimed that the most fundamental element of an ISS of an organization is an ISS awareness program, which is developed to enhance the behaviour of employees to ensure high level of security of both information and information assets of an organization. Furthermore, Lehrfeld, et al., (2013) suggested that an ISS awareness training program should be delivered by utilizing basic techniques such as training campaigns, use of video, case studies and related material.

The training programs whereas give benfits to an organization, conversely, these are also subjected to various lossess and costs in terms of effort, time & money (Shinder, 2013). Another disadvantage, identified by Papagiannakis (2012), is the gap between the theory and practice in seveal areas of ISS awareness. The author stated that there are still number of issues in ISS awareness, which are vague in practice and create challenges for organizations and IS professionals in the implementation of an training program (Papagiannakis, 2012). Hence, it has been depicted that the success of an ISS awareness training program should be based on fully analysis of organizational environment including structure, culture, goals, and targets to reduce the risk of facing the disadvantages associated with ineffective ISS awareness training programs.

D. General Deterrence Theory

GDT (General Deterrence Theory) is another ISS awareness approach that motivates employees and increases their awareness about using IS securely in their organization. According to D'Arcy, et al. (2009), GDT specifically focuses on the area of ISS behaviour of the users. Based on the behaviour of IS users, GDT suggested that unlawful and unethical attitude and behaviour of IS users can be managed and controlled by the threat of authorization which are certain, severe, and quick (D'Arcy et al., 2009). Moreover, from the notion of Schuessler (2009), it is depicted that GDT is effective to build up the positive behaviour of users toward the secure use of IS and the data stored in certain IS. Additionally, the author explained countermeasures as education, training, backups, reprimands, and so on that can be served as the approach to eliminate or mitigate such risks (Schuessler, 2009). In contrast, it is highlighted that in the ISS awareness, IS users should be aware of the security measures, preventive based security measures, and deterrent based security measures (Vaidyanathan & Berhanu, 2012). This would allow the employees to transfer the security information that ultimately meet with the security requirement of certain organization. This would overall represent the success of implemented security program (Figure 1).

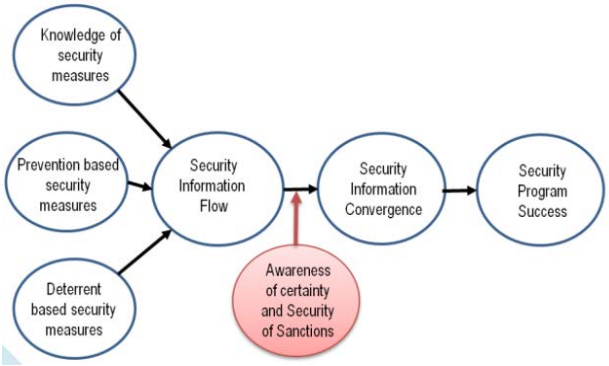

Figure 1 – General Deterrence Theory

Whereas GDT received great importance in literature, similarly the theory is criticized by several critiques. For instance, Lupovici (2010) stated that GDT has a lack of political component to motivate the employees and has strategic vulnerabilities which push the leaders to act aggressively if any IS users use IS in wrong way (Lupovici, 2010). Similarly, Piquero, et al. (2011) argued that short challenges with full scale attacks are difficult to deter since the theory is inefficient in terms of increasing awareness about taking immediate actions when any emergency or

unexpected attack take place in information system (Piquero et al., 2011). Hence, it is depicted that whereas the use of GDT identified effective as an ISS awareness approach, in contrast, there are some lacking areas due to which the theory cannot be applied effectively in every organizational setting.

The Table 1 highlights summarizes the findings from the literature by highlighting the limitations in each approach of IS security awareness.

Table I. Comparison of Information System Security Awareness Approaches

Approach	Limitations	Reference
ISACM	- Focus on awareness only - Lack of applicability with all organizations - No practical implications	(Poepjes & Lane, 2012)
Policies and Standards	- Lack of capability to work as exclusive approach - Complexities - Provides instructions only - Lack of technical information i.e. steps to be followed	(Haeussinger & Kranz, 2013; Bulgurcu et al., 2010)
Training Program	- Mainly applicable for small organizations - Lack of focus toward management - Lack of focus toward behaviour competence and clarity	(Karjalainen & Siponen, 2011; Lysenko, 2012; Shinder, 2013)
GDT	- Lack of Strategic focus - Lack of focus awareness of management - Inefficient toward increasing awareness about taking immediate actions	(Alanezi & Brooks, 2014; Lupovici, 2010; Piquero et al., 2011)

From the discussed literature, it is summarized that the existing theories and models whereas focusing on awareness or behaviour of the users toward using IS and ensuring its security, on the other hand, these models have been identified with the lack of technical aspects and practical implications, which is a question mark on the IS literature aspect which is missing while transferring awareness to the IS users. The significance of technical aspects of ISS awareness cannot be neglected. It is because, the use of IS widely based on the technical aspects; for instance, two people cannot communicate or transfer information to each other without having understanding about the system processing and the way certain technology transfer information from one end to another end. It is essential for IS users to be aware of the mechanism behind sending and receiving information to each other because sometimes unexpected threats could attack the system while two or more people communicating with each other. Therefore, it is vital for the organizations to focus on this area especially when they come to increase the awareness of IS users.

Moreover, in case of law enforcement agencies especially in the UAE, this issue should consider at priority because such kind of public sectors are more sensitive and require special attention to protect the information assets. However, in literature, no such study or research has been identified in context of the UAE law enforcement agencies to protect their systems. Since, UAE is one of the Arab countries which have different culture and values based on trust; therefore, it is essential to find how security of the systems is maintained in the organizations and how employees respond to it.

IV. METHODOLOGY

Since this study sheds light on the awareness among the employees in the UAE law enforcement agencies since they are responsible for the protection of homeland as well as the public data and information due to which the high level of security have to be ensured, a self-administered questionnaire were utilized to target the IS users of all levels who are responsible of maintaining security level in those agencies. For this purpose, a consent form was sent to the Ministry of Interior and permission was granted to distribute and collect the questionnaire from the UAE law enforcement agencies. Besides that, the GDT has been used as a foundation in this study. Depending on the different variables or important aspects of the theory, the researcher has formed questions in the survey process which also covers the information system security awareness approaches.

The researcher has chosen the survey questionnaire process to collect the primary data or quantitative data. The survey was done with the selected employees working in different UAE law enforcement agencies located in seven emirates which includes Abu Dhabi, Dubai, Sharjah, Ajman, Ras Al Khimah, Um Alquain and Fujairah. 500 questionnaires were distributed in total among the employees. The samples of the study following a probability random sampling technique. Out of 500 questionnaires, 58 questionnaires were excluded from the study due to incomplete data, while remaining 442 questionnaires are included in the study with a response rate of 88.4%. The profile of respondents is illustrated in Table II. According to Table II, most of the respondents were Policeman (48.19%) in the age group of 31-35 years (35.07%), with Master's degree (39.60%) and UAE nationality (65.15%) having experience of 1-5 years (30.55) in the UAE law enforcement agencies.

In the data collection process (survey), respondents were participated voluntarily as at the beginning of the survey, respondents were explained about the research purpose as well as allowed to leave or skip any question posed to them (Silverman, 2013).

The survey questionnaire designed for the study consisted of two parts. The first part was about the demographic status of the respondents including position, experience, age, education and ethnicity. The second part of the questionnaire was based on the five-point Likert scale, ranging from (1) "Strongly Agree" to (5) "Strongly

Disagree". The data collected has been analysed using statistical analysis approach whereas descriptive statistics was performed to present the findings (Bryman and Bell, 2011). In order to operationalize the constructs taken from literature, survey questionnaires were developed. However, necessary changes were made in wording to meet with the context of this study. Therefore, Table III shows the changes and modification in wording that has been made to meet with the requirements of this study.

Finally, for the analysis of quantitative or survey data, descriptive analysis was applied in order to understand the level of awareness among the employees or IS users in the UAE law enforcement agencies. Both central tendency and measure of dispersion were computed using SPSS Version 20 to conclude the findings (Braun and Clarke, 2006). In the end, quantitative results were discussed together with the support of literature review.

V. RESULTS AND DISCUSSION

In this section, the analysis of survey data is presented. The study was conducted to cover four main sections that are the information system security awareness, its policies and procedures, purpose of training and security awareness and GDT. The GDT was tested and the variables like preventive measures, ethical behaviour and individual's responsibilities were related to it. The rest two covered the other secondary concepts that were discussed in the study depending on the studies of previous scholars. The above-mentioned variables of the model have been used in the survey questionnaire process in a Likert scale to collect data and ensure whether the employees are properly trained or not and are aware of the awareness programs. The findings obtained from the study indicated various factors that influence the perception and behaviour of IS users within the UAE law enforcement agencies in terms of using the system. The findings are very much aligned with the discussed literature.

All the gathered data through survey were analysed and studied thoroughly and then classified in various categories to find different patterns as well as interpreted accordingly (Braun & Clarke, 2006). These categories are given in Table III:

Table II – Profile of Survey Participants

	N	*%*
Position		
Officer	62	14.03
Policeman	213	48.19
Manager/Executive	74	16.74
Other Positions	93	21.04
Experience		
<1 year	51	11.54
1-5 years	135	30.55
5-10 years	102	23.08
10-15 years	119	26.93
>15 years	35	7.90
Age		
< 25 years	47	10.64
25–30 years	129	29.18
31-35 years	155	35.07
36-40 years	76	17.19
> 40 years	35	7.92
Education		
High School	28	6.33
College	89	20.13
Graduate	124	28.05
Master's	175	39.60
Doctorate	26	5.89
Ethnicity		
Arab – Emirati	288	65.15
Arab - Non-Emirati	154	34.85

Table III – Construction of Survey Items from Literature

Categories	Survey Items
Individual Responsibility (Haeussinger & Kranz, 2013)	1. I have lack of awareness about using IS securely. 2. Organization offers proper training to the employees relating to securely use IS 3. Employees are provided with ISSA program at least once in a year to develop sense of responsibility among them
Policy Implications & Familiarity (Bulgurcu et al., 2010)	4. Organization has effective policies for ISS which is followed by everyone 5. Organization has documented guidelines about using IS 6. I can easily understand the ISS guidelines and policies and its implications
Ethical Behaviour (Levin & Klev, 2002; Kruger & Kearney, 2006; Bulgurcu et al., 2010)	7. I feel confident to share my username or password with the colleagues as I trust them a lot 8. In the organization, trustworthy attitude of IS users let them share their confidential information 9. Culture influences the ISS in the organization
Protective Measures (Baranowski et al., 2003; Kruger & Kearney, 2006)	10. Security tools and measures i.e. Strong Password, policies, software etc. are satisfactory integrated with IS of the organization 11. Organization's management team is regularly engaged with ISS to protect it at high level. 12. Organization uses international standards i.e. ISO 27001 for effective ISS management.
Employees Capabilities (Ajzen, 2011; El-Haddadeh et al., 2012)	13. The organization supports the awareness programs that are beneficial for ISS 14. I am aware of procedures and processes that can handle an unexpected ISS breach so that I can handle emergency situation. 15. I need to learn new skills and so that I become capable of using IS securely.

The following sections discuss the indicators of survey results:

i. Individual Responsibility

Individual responsibility is related to the behaviour of individuals towards ensuring ISS within the UAE law enforcement agencies. Table IV summarizes descriptive statistics of the responses obtained from the opinion of the respondents against first category 'individual responsibility', while Figure 3 shows the graphical representation of the results.

Table IV – Descriptive Statistics of Survey Items Related to Individual Responsibility

	Statement 1	Statement 2	Statement 3	Average
Mean	4.00	3.80	2.68	**3.49**
Median	4.00	4.00	2.00	**3.33**
Mode	5.00	5.00	1.00	**3.67**
Standard Deviation	1.28	1.27	1.64	**1.40**

The average value of Mean of all three statements is 3.49, which lies within the disagree agree scale, so it can be said that average respondents are not agreed with the given statements and found with lack of awareness and training practices related to ISS in the UAE law enforcement agencies. Besides, median is shown as 3.33, which revealed that 50% values lies within disagree scale of measures while the most repeated values has also been found on same scale as 3.67. Finally, the standard deviation (1.40) lies within the mean value therefore it can be said that the data has little variation.

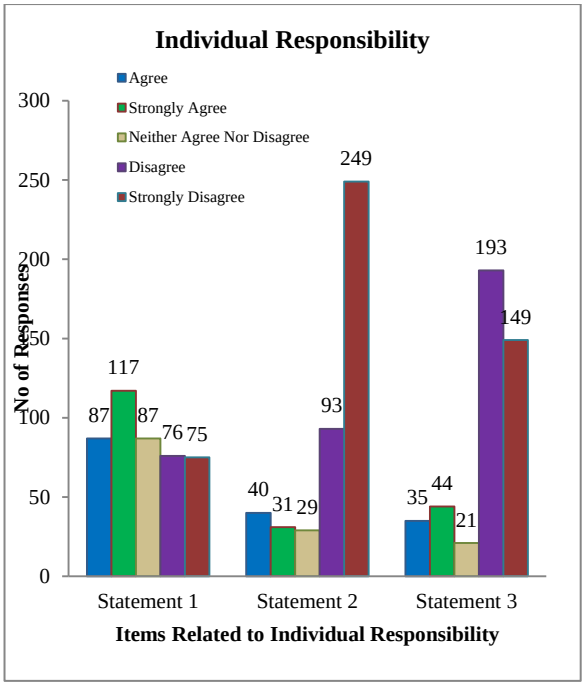

Figure 2 – Individual Responsibility

The data obtained from the survey revealed the facts about ISS in the UAE law enforcement agencies. Overall, the employees have been identified with less responsible behaviour toward ISS, which is still a challenge to the organizations. For example, employees show careless behaviour while using the systems i.e. share their username and password. Moreover, it is also revealed that only few people in the organization takes full responsibility as they are provided with the proper training, but most of the employees are not provided with the ISS training due to which they are not able to take the responsibility of ISS. Thus, the GDT can be applied here as a suggestive measure through which the researcher suggested that the staffs should take proper individual responsibilities to manage and control the threats of authorization. Besides that, they should also be provided with proper education and training regarding preventive based security measures as per the theory is concerned.

ii. Policy *Implications* & Familiarity

Concerning the policies and their implementation, it is found that the agencies have various policies for ISS, but the level of employees' awareness is very low. Most of the employees ignore or they do not know about the importance of security policies. They take it loosely and no practical implementation of those policies has been found throughout the organization. Table V summarizes descriptive statistics of the responses obtained from the opinion of the respondents against second category 'policy implication and familiarity', while Figure 3 shows the graphical representation of the results:

Table V – Descriptive Statistics of Survey Items Related to Policy Implication and Familiarity

	Statement 4	Statement 5	Statement 6	Average
Mean	3.66	2.22	3.62	**3.17**
Median	4.00	2.00	4.00	**3.33**
Mode	5.00	1.00	5.00	**3.67**
Standard Deviation	1.48	1.37	1.51	**1.45**

The average value of Mean of all three statements is 3.17, which lies within the disagree agree scale, so it can be said that average respondents are not agreed with the given statements and found with lack of familiarity with implemented policies and guidelines related to ISS in the UAE law enforcement agencies. Besides, median is shown as 3.33, which revealed that 50% values lies within disagree scale of measures while the most repeated values has also been found on same scale as 3.67. Finally, the standard deviation (1.44) lies within the mean value therefore it can be said that the data has little variation.

It is evaluated that employees in the UAE law enforcement agencies cannot understand the policies and guidelines being implemented by the organization. Since the unethical behaviour like sharing of passwords is a clear example of breach of policies and standards. It is also confirmed by the respondents that the organizations has policies and standards but these are not followed by the employees, which might be due to the lack of awareness of employees. Besides, the employees in the organizations also face

difficulty in understanding the guidelines as reported by many respondents in Figure 3 under the statement 6.

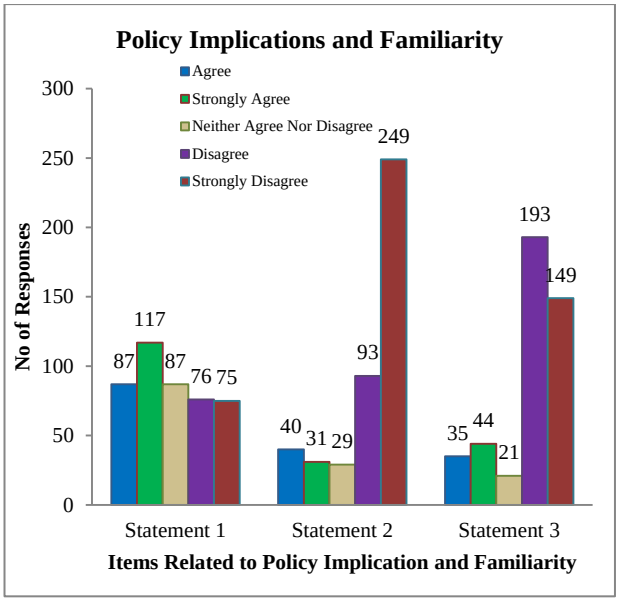

Figure 3 – Policy Implication and Familiarity

iii. Ethical Behaviour

In previous statements, employees revealed that they have lack of awareness about protecting the systems. In terms of security matters, sharing passwords and usernames is considered unethical because it is dangerous for the overall efficiency of the organization and may lead to leakage of confidential information. Globally, sharing or distributing password or username is unethical and all the standards and policies are not allowed to anyone or to share their passwords or usernames (Peltier, 2016). Similarly, the sharing of password or username among the employees in the UAE law enforcement agencies is unethical practice, which is due to their culture and trust factor, as shown by the respondents in Figure 4.

Table VI – Descriptive Statistics of Survey Items Related to Ethical Behaviour

	Statement 7	Statement 8	Statement 9	Average
Mean	2.20	2.35	2.11	**2.22**
Median	2.00	2.00	1.00	**1.67**
Mode	1.00	2.00	1.00	**1.33**
Standard Deviation	1.47	1.412	1.56	**1.48**

The average value of Mean of all three statements is 2.22, which lies within the 'agree' scale, so it can be said that average respondents are agreed with the given statements and found with unethical behaviour within UAE law enforcement agencies. Besides, median is shown as 1.67 that is also closed to 2 revealed that 50% values lies within 'agree' scale of measures while the most repeated values has also been found between 1 and 2 on same scale as 1.48. Finally, the standard deviation (1.48) lies within the mean value therefore it can be said that the data has little variation.

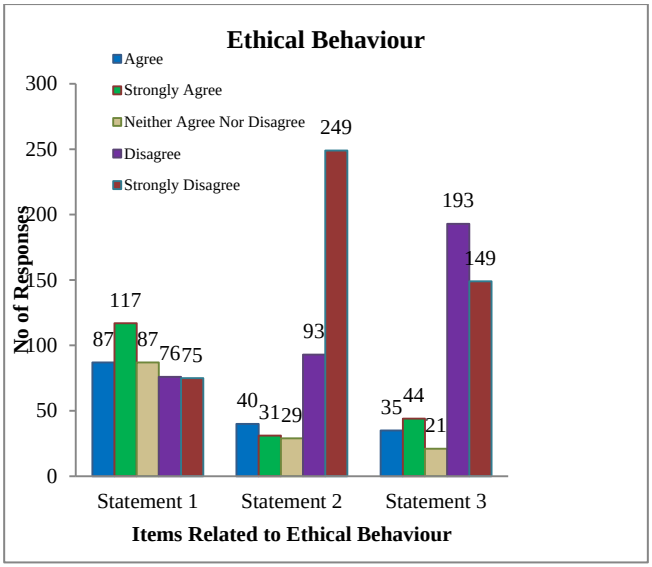

Figure 4 – Ethical Behaviour

Most of the respondents claimed that the organization has culture of trust, which allow them to share their username and password and lead to the breach of instruction that employees supposed to follow. This trusted culture also increases the chance of resistance, which might be a big threat to ISS of the organizations. In this context, the GDT principles can be compared where the individuals are motivated through security awareness program to show ethical and secure behaviour towards the organization to avoid risks or threats. In association to this, the researcher has included the following question in the survey process.

iv. Protective Measures

As a protective measure, it is found that various measures are implemented in the UAE law enforcement agencies to protect their system. For example, they have strong password like a mix of numbers, upper and lower case letters, and symbols, software, policies, standards, etc. However, it is the fact that all efforts fail if the employees show unethical behaviour and share their passwords or usernames openly. Therefore, in this case, these protective measures are completely useless. Besides, the polices and standards followed by the organization also work as a protective measure to protect the confidential information, but sadly, employees are not align with these policies due to lack of awareness and therefore strong actions are need to be taken to increase overall security. All these arguments are summarized in Figure 5.

Table VII – Descriptive Statistics of Survey Items Related to Protective Measures

	Statement 10	Statement 11	Statement 12	Average
Mean	2.21	2.04	3.79	**2.68**
Median	2.00	2.00	4.00	**2.67**
Mode	1.00	1.00	5.00	**2.33**
Standard Deviation	1.248	1.277	1.269	**1.26**

The average value of Mean of all three statements is 2.68, which lies within the 'agree' and 'neither agree nor disagree' scale, so it can be said that average respondents

are neither agreed nor disagreed with the given statements and found with the facts that the protective measures are being implemented in the UAE law enforcement agencies but are not followed by the users of the systems. Besides, median is shown as 2.67 that is also closed to 3 revealed that 50% values lies the same while the most repeated values has also been found between 2 and 3 on same scale as 2.33. Finally, the standard deviation (1.26) lies within the mean value therefore it can be said that the data has little variation.

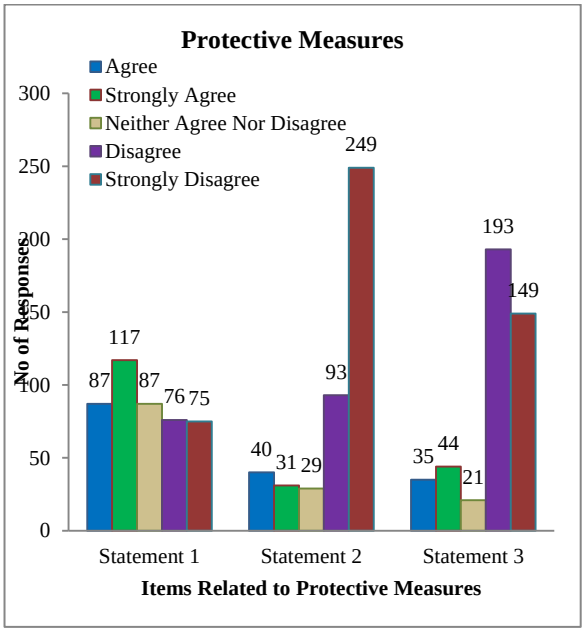

Figure 5 – Protective Measures

It is also found that the security agencies implement ISO 27001, which is one of the best standards in the ISO family that details the requirements for IS management system (ISMS) and based on the people, processes and IT systems by applying a risk management process (Peltier, 2016). However, the results revealed that not all the employees are aware about the integrated ISO standards and related guidelines. It is also confirmed that the organizations are doing its best for ISS, but the low awareness among employees increases the threat to the system. In connection to GDT, it can be further interpreted that as per the protective measures of Information System Security, the firms should educate or train the staffs with security measures and deterrent based security measures to manage and control the threats.

v. Employees Capabilities

In this context, relatively low or no capabilities among employees in terms of protecting the systems from unexpected threats and attacks has been observed. The respondents shared that whenever any employee has been hacked or attacked by the viruses, he or she cannot fix it unless getting help from the specialized department of IT. This indicates the careless behaviour and lack of awareness and capabilities among end-users about protecting the systems. Similarly, several facts have been revealed during the survey that is summarized in Figure 6.

Table VIII – Descriptive Statistics of Survey Items Related to Employees Capabilities

	Statement 10	Statement 11	Statement 12	Average
Mean	3.59	3.38	2.71	**3.23**
Median	4.00	4.00	2.00	**3.33**
Mode	5	5	1.00	**3.67**
Standard Deviation	1.586	1.476	1.638	**1.57**

The average value of Mean of all three statements is 3.23, which lies within the 'neither agree nor disagree' and 'disagree' scale, so it can be said that average respondents are neither agreed nor disagreed with the given statements and found with the facts that they have lack of capabilities to protect the systems in the UAE law enforcement agencies. Besides, median is shown as 3.33, between 'neither agree nor disagree' and 'disagree' scale, also revealed that 50% values lies the same scale while the most repeated values has also been found between 3 and 4 on same scale as 3.67. Finally, the standard deviation (1.57) lies within the mean value therefore it can be said that the data has little variation.

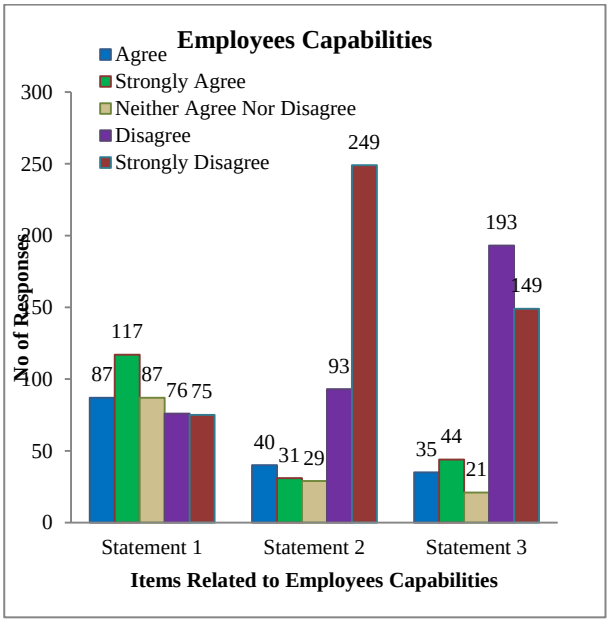

Figure 6 – Employees Capabilities

It is further depicted that in the UAE law enforcement agencies, employees especially outside the IT department have lack of capabilities and abilities in terms of addressing unexpected threats to ISS. Therefore, employees need more awareness and capabilities to deal with unexpected threat because more awareness allows them to handle and eliminate the security threats.

VI. DISCUSSION

It is evident that each program or a framework has its shortcoming and similarly the UAE law enforcement agencies are not exempted from it. With the help of the findings, it has been recognized that for ISS, agencies are performing at their best level, but the workforce failed in securing the systems effectively and proficiently, which is

unquestionably a crucial challenge for the security agencies.

The results of study provide support to the theories and the previous findings discussed in previous sections. The overall support of discussed literature towards the survey findings is relatively high with the considerable similarity index among the opinion of respondents with the supported mean value of each category Individual Responsibility (3.49), Policy Implications and Familiarity (3.17), Ethical Behaviour (2.22), Protective Measures (2.68) and Employees Capabilities (3.32). This is quite acceptable findings when it comes to compare with the findings of previous authors on ISSA including Bulgurcu et al. (2010) and Haeussinger & Kranz (2013) who found the mean value of Individual Responsibility, Policy Implications & Familiarity, Ethical Behaviour, Protective Measures and Employees Capabilities as 6.05, 5.96, 6.00, 6.06 and 5.48 respectively. It is suggest that the discussed theories and models as well as previous studies are capable of explaining the fact that Individual Responsibility, Policy Implications & Familiarity, Ethical Behaviour, Protective Measures, and Employees Capabilities are the key factors through which ISSA level of the individuals can be determined. The following findings can also be connected with the applied theory that is GDT. As per the theory, the firms should provide proper training and education to the employees so that they can show secured behaviour in using the tools and control threats. This is related to ethical behaviour as interpreted in the results of the study. Further, the theory indicates that an individual should take own responsibilities to make sure that the information system used in the firm is secured. This is related to individual responsibility of the study. Other than these, as per the results of the study, the individuals should be aware of proper security measures like deterrent based security measures so that the threats can be controlled and the firm can get rid of risks.

In addition to the above, number of insights relevant to the developed categories have been found that are much similar to the study conducted in context of the UAE law enforcement agencies. These findings would help in understanding the current level of awareness among the employees as well as ensure that the security agencies in the UAE needs to have a proper framework so is to deal with identified issues.

First of all, concerning to Individual Responsibility among employees within the UAE law enforcement agencies, it is acquired that employees are intended to show the negative attitudes due lack of awareness programs and lacks of proper training. This fact is supported by the findings of Albrechtsen and Hovden (2010) as they found incompetence and lack of awareness of users as the biggest ISS problem and argued that users without awareness cannot give the value to the risks associated with their wrong acts and inherent actions. The authors also emphasized on the requirement and essentiality of ISSA program in an organisation to overcome the identified concern. Same as, in case of the UAE law enforcement agencies, it can be said in light of the findings that awareness among the employees and their positive attitude can bring the positive change in overall security of the systems and the data stored. In this scenario, Deterrence Theory supported that security breaches and negative attitude of the employees within the organization are the key threat to IS security (Loughran et al., 2012; Jing & Pengzhu, 2011). Thus, UAE law enforcement agencies would have choice to identify the weakness in employees' attitudes with the help of internal organizational controls and determined detection actions.

Besides, concerning to Policy Implications & Familiarity within the UAE law enforcement agencies, it is examined that the practice of sharing password or username is a clear sign of lack of employees' understanding about using security guidelines and policies to secure their systems and data. According to Haeussinger & Kranz (2013), employees' familiarity or awareness about ISS policies is of great importance especially when it comes to protect the systems. It is because policies and guidelines develop the knowledge among the employees, which help them in dealing with the unexpected threats. Similarly, Bulgurcu et al. (2010) also supported this fact and highlighted knowledge about policies and guidelines as a key factor in securing the systems. Therefore, it can be said that awareness regarding ISS is mainly concerned with educating the employees, which should be particularly relevant to the security issues as well as to develop the sense of security whether it is right and wrong (Baranowski et al., 2003).

The results obtained in context of Ethical Behaviour support the fact that culture and trust have considerable influence on maintaining the security of organizational information assists and the systems. Since, survey results highlighted the culture and trust as the key factors behind the security breaches. In the UAE law enforcement agencies, there is a culture of trust that allows employees to share their username or password openly with their sub-ordinates. This situation ultimately welcome to unwanted circumstances by affecting the security of the systems. As Nicolaisen (2010) in his study supported that employees' involvement in risky behaviour such as sharing passwords, connecting external devices, or neglect to consider security in their daily routines always put the systems at risk.

Security behaviour in line with Protective Measures within the UAE law enforcement agencies, it is obtained that security controls are constantly implemented in the organizations in identifying and authenticating users, but the unethical use of the systems by the employees is a sign of security breaches as well as determined that the confidential information can be access and transmitted openly without any fear, which ultimately increases the risk of manipulation of sensitive information. In literature, the importance of ISS is considered as a key area to maintain security of information and prevent organization from any sort of illegal security scandals as well as to provide strong support to the entire organization's structure (Andreas, 2003). In this case, a legal activity of preventing and rectifying a wrong and enforcing a right can be adopted by the UAE law enforcement agencies as this will help in taking effective actions to prevent IS from any sort of threat. Additionally, the security agencies can adopt any

internal (suspensions, fines or terminations) or external remedies (force to follow policies or procedures) to protect their system (Piquero et al., 2011).

Finally, concerning to Employees Capabilities in the UAE law enforcement agencies, it is found that employees do not intentionally breach the system security. Since, they have lack of awareness and capabilities, which lead to certain situation. Kaur and Mustafa (2013), in this instance, stated that ISS awareness means the capabilities and abilities of an organization or the users to protect the system from unexpected threats so that security of all data can be ensured. From this view, it can be said that only certain level of awareness and capabilities among the employees can protect the system adequately, while other technologies and measures will also become effective, if the users will have sufficient knowledge about using them (Banerjee & Murarka, 2013).

VII. PROPOSED MODEL AND RECOMMENDATIONS

Majority of researchers agreed with that ISS awareness is useful to successfully address ISS concerns and to ensure the reliability of an organization for securing its data resources (Banerjee and Murarka, 2013; Bulgurcu, et al., 2010). Based on the identified gaps and limitations in literature as well as the weak security awareness practices in the UAE law enforcement agencies, it is recommended to address the current issue by implementing the new model to secure the data resources. Therefore, a new model is developed and proposed to the security agencies which is called ''Information System Security Awareness and Behaviour Competence Model (ISSABCM)' as shown in Figure 7.

ISSABCM proposes that IS security awareness requires a proper system to ensure the high level of awareness and behaviour competence of IS users necessary to maintain the security of IS in an organization.

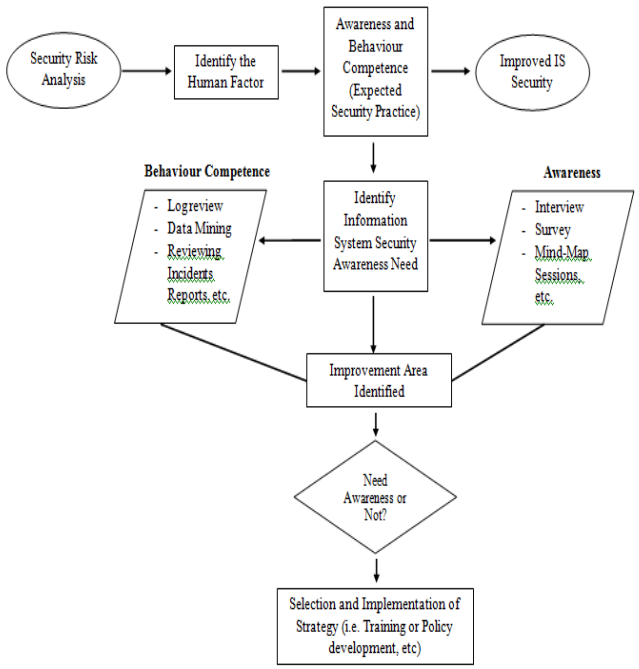

Figure 7 – ISSABCM

The model also illustrates that after the identification of the human factors that contribute to security risk, the awareness and behaviour competence stage comes. Awareness to IS users cannot be provided directly therefore identification of improvement areas is necessary before the implementation of any awareness program. The model further elaborate the techniques that can be used to identify the areas for awareness and behaviour competence, since awareness is different from the behaviour competence therefore individual strategies are allocated to each. Finally, after analysing the key issues and gaps, it become easy to develop the relevant strategies such as training program or policy development so that level of awareness can be increased along with positive behaviour competence toward using IS securely.

Hence, these elements of the model would address the gaps identified in earlier models and theories of ISS awareness. A checklist is also developed for this model by incorporating the elements from ISO 27002, so that the high level of security awareness would be ensured that meets with the international standards and regulations. This checklist is given in given in Figure 8.

By implementing the developed model, the UAE law enforcement agencies will able to overcome the security challenges mainly took place due to lack of employees' awareness working at different levels. Overall, the implementation of the suggested model would ensure the higher level of security of the systems and confidential data.

Information Security Awareness Capability Model Updated

ISO 27001 Control Standards	Stakeholder Grou	Awareness Importance					Awareness Capability					Awareness Risk
		Importance (influence) that awareness provides to the control for each stakeholder group. How much awareness is required?					Level of awareness being displayed by each stakeholder category					Highlight gap in required awareness - interface with risk assessment matrix
ISO 27002 List of Controls		None	Slightly	Moderate	Very	Extreme	None	Slightly	Moderate	High	Expert	**Overall Rating**
5. Security Policy												
5.1. Information Security Policies	**Objective:** To provide directions to the IT management and individual user for information security in order to meet with e-government security objective and relevant laws and regulations.											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
6. Corporate Security												
6.1. Internal Organization Level	**Objective:** To manage information security at internal level of the organization											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
6.2. External Parties	**Objective:** To manage information security of organization from external parties											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
7. Personnel Security												
7.1. Culture and Social Backgrouds Authentication Prior to Employement	**Objective:** To ensure the newly employed employees and their backgrounds are adequatly meets with organization's security standards											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
7.2. Deliver information security awareness programs	**Objective:** To manage information system security by providing adequate awareness training to personnel											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
8. Organizational Asset Management												
8.1. Responsibility of Assets	**Objective:** To achieve and maintain appropriate protection of organizational assets.											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
8.1. Information Classification	**Objective:** To ensure that information receives an appropriate level of protection.											
	Senior Management											High/ Medium/ Low/ None
	IT Staff											High/ Medium/ Low/ None
	End Users											High/ Medium/ Low/ None
9. Information Access Management												

Figure 8 - Checklist to Assess ISSABCM

VIII. CONCLUSION

This paper shed light on various ISS awareness approaches as well as evaluated the security behaviour and awareness level of the employees working in the UAE law enforcement agencies. It has been concluded with the fact that previously proposed approaches and models whereas worked successfully; on the other hand, these approaches have some limitations too, which highlighted the need to have a new model. Similarly, in case of the UAE law enforcement agencies, lack of awareness among employees has been identified as reported by the survey results. Based

on these facts, it is concluded that there is need to bring a newly approch to ISS awareness, which can be implemented in the security or law enforcement agencies in the UAE as well as at global level. Therefore, ISSABCM model has been developed and suggested which will help the security agencies in improving overall ISS by improving the level of awareness among the employees.

REFERENCES

[1] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2), 357-370.

[2] Ajzen, I., 2011. Theory of planned behavior. *Handbook Theory of Social Psychology* , p.438.

[3] Alanezi, F. & Brooks, L., 2014. *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT)*. UK: Brunel University.

[4] Albrechtsen, E. & Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security* , 29(4), pp.432-45.

[5] Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176-183.

[6] Andreas, P., 2003. Redrawing the line: borders and security in the twenty-first century. *International security*, *28*(2), pp.78-111.

[7] Bainbridge, D.I., 2011. *Introduction to Information Technology Law*. New York: Pearson Education, Limited.

[8] Banerjee, A.B. & Murarka, P.D., 2013. An Improvised Software Security Awareness Model. *International Journal of Information, Communication and Computing Technology, ,* 1(2), pp.43-48.

[9] Birkinshaw, P., 2010. *Freedom of Information: The Law, the Practice and the Ideal*. Cambridge : Cambridge University Press.

[10] Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp.77-101.

[11] Bryman, A. & Bell, E., 2011. *Business research methods 3e*. Oxford University Press.

[12] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), pp.523-548.

[13] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

[14] Calder, A., 2012. *Implementing information security based on ISO 27001/ISO 27002*. New York: Van Haren.

[15] Case, D.O., 2012. *Looking for information: A survey of research on information seeking, needs and behavior*. New Jersey : Emerald Group Publishing

[16] Chen, H., Wang, F.Y. and Zeng, D., 2004. Intelligence and security informatics for homeland security: information, communication, and transportation. *IEEE Transactions on Intelligent Transportation Systems*, *5*(4), pp.329-341.

[17] Chen, Y., Paxson, V. and Katz, R.H., 2010. What's new about cloud computing security. *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, *20*(2010), pp.2010-5.

[18] CJIS, 2016. *CJIS Security Awareness Training*. CJIS.

[19] Cordella, A. & Iannacci, F., 2010. Information systems in the public sector: The e-Government enactment framework. *The Journal of Strategic Information Systems* , 19(1), pp.52-66.

[20] Corona, C.O., 2010. *Information Security Awareness: An Innovation Approach*. England: Royal Holloway, University of London.

[21] Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioral information security research. *computers & security*, *32*, pp.90-101.

[22] Crowley, E., 2003, October. Information system security curricula development. In *Proceedings of the 4th conference on Information technology curriculum* (pp. 249-255). ACM.

[23] D'Arcy, J., Hovav, A. and Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), pp.79-98.

[24] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

[25] El-Haddadeh, R., Tsohou, A. & Karyda, M., 2012. Implementation Challenges For Information Security Awareness Initiatives In E-Government. *ECIS 2012 Proceedings. Paper 179*.

[26] Federal Office for Information Security, 2014. *BSI Standard 100-1 Information Security Management Systems (ISMS)*. [Online] Available at: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html [Accessed 25 Janury 2017].

[27] Haeussinger, F. & Kranz, J., 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. In *International Conference on Information Systems*. Milan, 2013. Georg-August-University Goettingen.

[28] He, Y. & Johnson, C.W., 2012. Generic security cases for information system security in healthcare systems. In *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*., 2012. IET.

[29] Herath, T. and Rao, H.R., 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), pp.154-165.

[30] Herold, R., 2010. *Managing an information security and privacy awareness and training program*. New York: CRC press.

[31] Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), pp.83-95.

[32] Information Commissioner's Office, 2014. *Information security (Principle 7)*. [Online] Available at: http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7 [Accessed 20 January 2017].

[33] ISO Directory, 2014. *Introduction To ISO 27006 (ISO27006)*. [Online] Available at: http://www.27000.org/iso-27006.htm [Accessed 15 January 2017].

[34] Jing, F. & Pengzhu, Z., 2011. Study on e-government information misuse based on General Deterrence Theory. In *8th International Conference on Service Systems and Service Management (ICSSSM)*., 2011.

[35] Kang, M.-C., 2013. *ecurity: Be Ready to Be Secure*. Florida: CRC Press.

[36] Karjalainen, M. & Siponen, M., 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), pp.518-55.

[37] Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518.

[38] Kaur, J. & Mustafa, N., 2013. Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In Research and Innovation in Information Systems (ICRIIS). In *2013 International Conference on Information System Security Awareness*., 2013. IEEE.

[39] Knapp, K.J. & Ferrante, C.J., 2012. Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management*, 13(5), p.67.

[40] Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), 493-508.

[41] Kouns, J. & Minoli, D., 2011. *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. New York: John Wiley & Sons.

[42] Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.

[43] Kruger, H. & Kearney, W., 2006. A prototype for assessing information security awareness. *Journal of Computers and Security*, 25(4), pp.289–96.

[44] Lebek, B. et al., 2013. Employees' information security awareness and behavior: A literature review. In *46th Hawaii International Conference on System Sciences*. Hawaii , 2013. IEEE.

[45] Lehrfeld, M.R. et al., 2013. Development of a Security Awareness Program to Reduce Security Breaches and Virus Outbreaks. In *46th Annual Conference*., 2013.

[46] Levin, M. & Klev, R., 2002. *Changes in practice: learning and development in organizations*. Bergen.

[47] Loughran, T.A., Pogarsky, G., Piquero, A.R. & Paternoster, R., 2012. Re-examining the functional form of the certainty effect in deterrence theory. *Justice Quarterly*, 29(5), pp.712-41.

[48] Lu, Y. and K. Ramamurthy, 2011. Understanding the link between information technology capability and organizational agility: An empirical examination. *Mis Quarterly*, pp.931-954.

[49] Lupovici, A., 2010. The emerging fourth wave of deterrence theory—Toward a new research agenda. *International Studies Quarterly*, 54(3), pp.705-32.

[50] Lysenko, V., 2012. *Proceedings of the 7th International Conference on Information Warfare and Security*. South Africa: Academic Conferences Limited.

[51] Meszaros, J. and Buchalcevova, A., 2017. Introducing OSSF: A framework for online service cyber security risk management. *Computers & Security*, *65*, pp.300-313.

[52] Missouri Police, 2012. *Security Awareness Training Guide For Chiefs Of Police*, Missouri Police.

[53] Myers, M.D. & Klein, H.K., 2011. A Set of Principles for Conducting Critical Research in Information Systems. *MIS Quarterly*, 35(1), pp.17-36.

[54] Nicolaisen, N., 2010. Maintaining Privacy and Security in a Pervasively Connected World. *Getting StartED with Netbooks*, pp.301-55.

[55] Papagiannakis, K., 2012. *An Overview of the Current Level of Security Awareness in Greek Companies*. Erasmus University.

[56] Parliament, U. & Committee, J., 2012. *The Committee's Opinion on the European Union Data Protection Framework Proposals*. UK: The Stationery Office.

[57] Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press

[58] Piquero, A.R., Paternoster, R., Pogarsky, G. & Loughran, T., 2011. Elaborating the individual difference component in deterrence theory. *Annual Review of Law and Social Science*, 7, pp.335-60.

[59] Poepjes, R. & Lane, M., 2012. An Information Security Awareness Capability. In *Australian Information Security Management*. Perth, Western Australia, 2012. Research Online.

[60] Ponemon Institute, 2010. *Ponemon Institute 2010 Access Governance Trends Surve*. Ponemon Institute.

[61] Puhakainen, P. & Siponen, M., 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4).

[62] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778.

[63] Richardson, R. and Director, C.S.I., 2008. CSI computer crime and security survey. *Computer Security Institute*, *1*, pp.1-30.

[64] Rose, N., 2000. Government and control. *British journal of criminology*, *40*(2), pp.321-339.

[65] Sanyal, S., Shelat, A. & Gupta, A., 2010. New Frontiers of Network Security: The Threat Within. In *Information Technology for Real World Problems (VCON), 2010 Second Vaagdevi International Conference*. Warangal, 2010. IEEE.

[66] Schuessler, J., 2009. *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses*. Ph.D. dissertation. Texas: University of North Texas.

[67] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.

[68] Shinder, D., 2013. Security Awareness Training: Your First Line of Defense. *WindowSecurity.com*, 12 June.

[69] Silverman, D., 2013. *Doing qualitative research: A practical handbook*. SAGE Publications Limited.

[70] Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). *Computer security: principles and practice* (pp. 978-0). Pearson Education.

[71] Vaidyanathan, G. & Berhanu, N., 2012. Impact Of Security Countermeasures In Organizational Information Convergence: A Theoretical Model. *Issues in Information Systems*, 13(2), pp.21-25.

[72] Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, 18(2), 101-105.

[73] Whitman, M.E. & Mattord, H.J., 2010. *Principles of information security*. New York: Cengage Learning.