International Journal on Emerging Technologies **11**(3): 1194-1203(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

Enhancing Information Security Awareness among Omani Public Sector Employees: A Pilot Study

Issam Al-Shanfari[1], Warusia Yassin[1], Raihana Syahirah Abdullah[2] and Gumma Magrisi[2]

[1]Ph.D. Student, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, MALAYSIA.
[1]Senior Lecturer, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, MALAYSIA.
[2]Senior Lecturer, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, MALAYSIA.
[2]Ph.D. Student, Faculty of Informatics & Computing, Universiti Sultan Zainalabdin (UniSZA), Terengganu, MALAYSIA.

(Corresponding author: Issam Al-Shanfari)

(Received 17 April 2020, Revised 12 June 2020, Accepted 22 June 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Awareness plays an important role in the field of information security (IS) due to its positive impact on staff adherence to security policies. With the development and increase in cases of information piracy and phishing attempts, the challenges inherent in protecting the information infrastructure of Omani public sector institutions are drastically increasing. Governmental networks are exposed to cyber-attacks due to lack of information security awareness (ISA) for many employees. Therefore, it is necessary to enhance security awareness for government units' employees to ensure best practices for systems users are achieved. The study follows a positivist philosophy and takes a quantitative approach applied through a survey distribution by used a self-administered questionnaire as an instrument of this research. The aim of this study is to validate the reliability of the questionnaire items to ensure that these items are ready to be used in a major survey of an adopting ISA model in Oman. The statistical analysis includes a skewness test, reliability analysis and correlation analysis. The theory of planned behaviour (TPB), protection motivation theory (PMT), and general deterrence theory (GDT), as well as the Triandis model (facilitating conditions), were applied as the theoretical backbone of the study's conceptual model. The results of this study showed that all construct items—subjective norms, perceived behavioural control, response efficacy, perceived vulnerability, perceived certainty of sanctions, perceived severity of sanctions, behavioural intention, actual behaviour, organizational support, and communication—have acceptable values of Cronbach's alpha test. Attitude showed excellent value. The results of this pilot study should be of interest to those interested in the field of IS. It also contributes to the literature on ISA and on promoting ISA in Oman.

Keywords: Enhancing Awareness, Information Security Awareness, Pilot Study, Survey.

I. INTRODUCTION

At the present time, information security (IS) is considered a major factor affecting the sharing and exchange of information between individuals, one that is becoming increasingly important among government institutions [1]. Because the databases of government units contain, in addition to administrative and financial data, huge amounts of information about citizens and businesses, much research shows that misuse of that information, which can result from a lack of IS awareness , may not only lead to a loss for government units, but can also harm citizens and businesses [2]. Common phenomena that result from a lack of employees' information security awareness (ISA) are the infection and destruction of government systems with viruses and malware, the disclosure of sensitive government information to unauthorized internal officials, the destruction or disabling of government networks and the shutdown of service.

The term IS refers to protecting information in general, protecting information systems from unauthorized access, use, modification, disclosure, perusal and disruption in order to maintain the confidentiality, integrity, availability and reliability of information [3], [4]. ISA is not just about instructions, but is an integrated process of training, education and awareness that enhances the focus of attention, makes employees knowledgeable about IS and aware of all regulations, laws and information security policies, thus enabling them to respond accordingly [5].The IS literature often indicates that the human component is always the weakest link in security; the gap between awareness and ideal security practices that must be followed is often the main factor which affects IS assets [6]. Some researchers indicate that internal users may be the problem and also the solution while implementing security policies within an organization; therefore, many security experts urge investing in both technical-based and human resource solutions in parallel in order to achieve success in IS [6-8].

This study is important because it is a continuation of our efforts to find the optimal solution to the problems of recurring security breaches referred to in our previous research [6]. It provides a novel model to enhance ISA among public sector employees in the Sultanate of Oman that takes into account the importance of utilizing the most successful psychological factors for positively influencing ISA. Hence, the purpose of this paper is to conduct a pilot study (survey) of Omani public sector institution employees' ISA on the one hand and to validate the items of the main research instrument (questionnaire) on the other .In this paper, a theoretical model is presented, followed by the methodology and research instrument of the study. The pilot study is presented in section five. Afterwards, the respondents' characteristics are presented, followed by reliability and Pearson's tests of the variables' relationships. The conclusion and ideas for future work are presented at the end of the paper.

II. THEORETICAL BACKGROUND

We propose the study model of ISA under three fundamental theories: theory of planned behaviour (TPB), protection motivation theory (PMT), and general deterrence theory (GDT). Furthermore, we support our proposed model with the Triandis model by considering the facilitating conditions that encourage individuals to behave in a certain way and to develop their behaviour. It is desirable to study enhancing ISA from different perspectives; incorporating TPB, PMT, and GDT into the proposed model makes it an integrative process concentrated upon control, prediction, motivation and deterrence. Many studies have used or referred to multiple psychological theories about the behaviour, perception and intention of an individual in the context of information technology. According to [4, 6, 7, 9 10], psychological theories such as PMT, TPB, GDT, and social cognitive theory (SCT) are the most widely used theories of applied behaviour in the context of ISA.

A. Theory of Planned Behaviour (TPB)

An individual is influenced by all the people who interact with his/her daily life; this effect extends to feelings, thoughts, behaviours and actions. TPB was proposed by Ajzen [11] and was developed from the theory of reasoned action (TRA), which describes that human behaviours change based on social influence. In clearer terms, if individuals evaluate a particular behaviour as positive (attitude) or if they believe that people important to them want them to do a certain behaviour (subjective norms), then these should guide them to higher intentions and they will be more likely to act on them in fulfilment of the desire of others [12].Some studies have shown that behavioural intention cannot be the exclusive determinant of actual behaviour, creating controversy regarding the relationship between behavioural intention and actual behaviour in cases where an individual's control of his or her behaviour is deficient. Ajzen [11] developed the theory by looking at perceived behavioural control in order to include involuntary behaviour in predicting the intention and behaviour of an individual. Constructs of TPB theory have been used in many studies related to information technology/security [4, 13, 14, 15, 16]. TPB is better in the case of controlling employee beliefs; therefore, all of its three constructs are utilized in this research due to its applicability to describing how employees participate in ISA and its greater consideration of social influences on technology use and adoption.

B. Protection Motivation Theory (PMT)

PMT was developed by Rogers [17] in order to assist in recognizing and understanding fear appeals. Receiving information about threats has an important role in an individual's awareness and cognition of risks. Rogers depended on cognitive processing and expectancy value theories to develop this theory, which made it a powerful theory providing a clear explanation for predicting behavioural intentions in adopting protective measures [18]. PMT consists of two main parts: threat appraisal and coping appraisal. Threat appraisal consists of two important factors, perceived vulnerability and perceived severity. In turn, coping appraisal comprises the three factors of self-efficacy, response efficacy and response costs. Various studies [13, 14, 19, 20] have applied PMT's constructs to demonstrate compliance with IS policies within organizations. Only perceived vulnerability and response efficacy are utilized in the integrated study's model because these two variables have a positive effect on the findings of the aforementioned studies.

C. General Deterrence Theory (GDT)

A precocious version of deterrence theory was invented by the philosophers Cesare Beccaria and Jeremy Bentham. It was based on the belief that people will seek to maximize enjoyable consequences, such as rewards, and reduce painful consequences, such as penalties [21]. GDT was originally used in criminology to reduce individuals' deviant behaviour. Lately, it has been successfully applied to the information technology/security environment [10, 16, 22, 23]. There are two central predictors included in the GDT, the perceived certainty of sanctions and the perceived severity of sanctions. Certainty indicates that a person believes that his or her criminal behaviour will be revealed, while severity refers to the belief that a person will be severely (harshly) punished if he or she actually commits criminal behaviour [24]. Therefore, the more certainty and severity a person has against illegal behaviour, the greater his or her level of deterrence from criminal acts. Since GDT relies on rational decision-making to deter crime or security breaches in the future [25], it is quite appropriate to utilise it to influence employees' decisions regarding adherence and compliance to IS policies and to increase their ISA. Both variables sanction severity and sanction certainty, are included in the study's model.

D. Facilitating Conditions

According to Triandis [26], facilitating conditions are objective and effective factors arising from the environment itself that are added to other factors in order to achieve a particular behaviour and make it easy to do. In the context of this study, we utilized two predictors as facilitating conditions, which are organizational support for and communication among employees of the Omani public sector in order to raise their awareness in the context of IS. Organizational support has proven to have a significant effect on knowledge sharing in the fields of IS [4] and communities of practice [27].

We believe that communication among employees regarding information security can work to harmonize and equate the methods used to manage human weaknesses on the one hand and between advanced technical security mechanisms on the other where the management of human consciousness is considered much too much late compared to the methods of advanced technology [28, 29]. Therefore, good communication is an encouraging factor in the success of ISA, [30] one through which employees can gain many efficient skills and reduce incorrect assumptions about individuals, beliefs and their motivations.

III. METHODOLOGY

Through this study, we seek to increase and diversify research on the management of the human element in terms of IS while increasing awareness and knowledge of IS as an effective approach in reducing the risk of security breaches that threaten the integrity of information. TPB, PMT, GDT and facilitating conditions helped us to conceptualise the success factors for raising ISA in Omani public sector organizations. Hence, the study follows a positivist philosophy and takes a quantitative approach applied through a survey distribution. Fig. 1 shows the study's methodology flowchart.

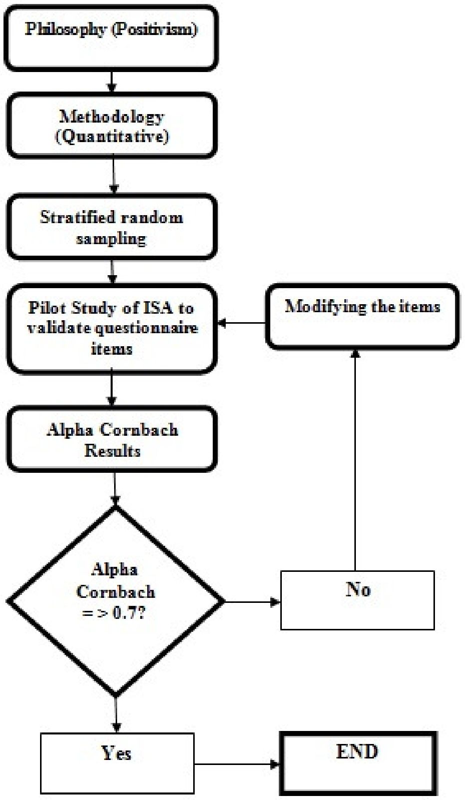
Philosophy (Positivism)
Methodology (Quantitative)
Stratified random sampling
Pilot Study of ISA to validate questionnaire items
Modifying the items
Alpha Cornbach Results
Alpha Cornbach = > 0.7?
No
Yes
END

Fig. 1. Research Methodology.

The main objective of conducting a pilot study is to validate the reliability of the survey's (research instrument) items [31]. This in turn paves the way for conducting the main survey after ensuring that the items are ready and appropriate.

The study targets the public sector employees in Omani institutions because the public sector is considered one of the most vital and necessary sector in Oman; it is the largest sector in terms of number of employees, with a total of 175,868 employees [32]. The researcher distributed 110 questionnaires to employees of a chosen sample that closely resembles the target population of this study. Eighty-seven questionnaires were retrieved and validated for statistical analysis, a 79% rate of response.

IV. THE STUDY'S QUESTIONNAIRE

As mentioned above, this study used a quantitative approach. Since a survey is an appropriate method for examining factors and testing hypotheses [31], it is the method utilized in this study. The research instrument consists of two main sections; the first one is respondents' characteristics and includes seven (7) questions, while the second contains questions about the factors (predictors) of the proposed model with a total of (64) questions.

In the questionnaire, the dependent variables behavioural intention and actual behaviour have seven (7) and nine (9) items, respectively. For the three TPB variables, attitude and subjective norms have six (6) items each, while perceived behavioural control has only five (5) items. The two PMT variables, perceived vulnerability and response efficacy, have five (5) items each. GDT includes two variables, perceived certainty of sanctions with five (5) items and perceived severity of sanctions with six (6) items. In addition to the items that are based on psychological theories, two variables of facilitating conditions were employed, organizational support and communication, each of which has five (5) items. Table 1 shows the model's factors.

Table 1: The model's factors.

Variable	Items	Ref.
Behavioural Intention	7	[4, 33]
Actual Behaviour	9	[4, 33]
Attitude	6	[4, 13]
Subjective Norms	6	[4, 13, 33]
Perceived Behavioural Control	5	[4, 13, 33]
Perceived Vulnerability	5	[13, 14]
Response Efficacy	5	[14]
Perceived Certainty of Sanctions	5	[33, 34, 35]
Perceived Severity of Sanctions	6	[33, 34, 35]
Organizational Support	5	[4, 26 , 27]
Communication	5	[28, 29, 30]

In addition to the above, a skewness test was used in order to check the data for normality. The value of skewness must be within (±1 and ±2) so that the skewness of a certain variable is determined by division of the skewness statistic with std. error. Table 2 shows that the questionnaire variables were found to be statistically significant. The researcher followed the guidelines that suggested a cut-off critical value of ±2.58 [36]. From Table 2, it is obvious that the value of skewness for each variable was within the given range (±2.58). The descriptive analysis indicates that skewness values show an almost normal distribution and ranged from 0.717 to 1.906.

Table 2: Skewness results.

Variable	Skewness / Std. Error	Result
Behavioural Intention	.185 / .258	.717
Actual Behaviour	-.416 / .258	1.612
Attitude	-.430 / .258	1.666
Subjective Norms	-.328 / .258	1.271
Perceived Behavioural Control	-.462 / .258	1.792
Perceived Vulnerability	-.192 / .258	.774
Response Efficacy	-.355 / .258	1.375
Perceived Certainty of Sanctions	-.331 / .258	1.282
Perceived Severity of Sanctions	-.290 / .258	1.142
Organizational Support	-.492 / .258	1.906
Communication	-.411 / .258	1.590

V. PILOT STUDY

A pilot study is an experiment or a trial conducted on a very small sample of the target population before the main survey takes place [36]. According to Hair et al. [36], there are several reasons why researchers conduct pilot studies. The first is to determine if there are any logistical problems that may occur during data collection, and the second is to develop research instruments and examine their adequacy for collecting data. A third reason is to determine whether the sampling technique and method are effective. The goal of this pilot study is to improve the study's questionnaire if needed, test the question sequencing and wording, check familiarity with respondents, estimate the time required to complete the test and perform a pre-test statistical analysis.

Since the study population exceeds 175000, 110 questionnaires were distributed to respondents over a period of 10 working days. Eighty-seven questionnaires were retrieved and validated for statistical analysis, a79% rate of response. To determine the reliability of the questionnaire scale for the collected data of this pilot study, SPSS Statistics 23 software was used.

VI. RESPONDENTS' CHARACTERISTICS

The purpose of demographic factors used in a questionnaire is to verify the collected data. Our questionnaire involved seven demographic factors: gender, age, position, work experience, education, level of ISA and organization. Table 3 presents the demographic factors of the participants.

Table 3: Respondents' characteristics.

Measure	Items	Frequency	Percent
Gender	Male	50	57.5
	Female	37	42.5
Age (in years)	25 or Less	0	0
	26 – 30	7	8.0
	31 – 35	25	28.7
	36 - 40	23	26.4
	Above 40	32	36.8
Position	Employee	21	24.1
	Specialist	25	28.7
	Technician	18	20.7
	Chief-Employee	9	10.3
	Management	6	6.9
	Other	8	9.2
Experience (in years)	1 - 2	3	3.4
	3 - 5	3	3.4
	6 - 10	22	25.3
	Above 10	59	67.8
Education	Diploma	6	6.9
	High Diploma	10	11.5
	Bachelor	48	55.2
	Master	21	24.1
	PhD	2	2.3
Level of ISA	Elementary	14	16.1
	Intermediate	53	60.9
	Advanced	20	23.0
Organization	Education	54	62.1
	Health	2	2.3
	Service	15	17.2
	Other	16	18.4

In Fig. 2, males represented the largest number of respondents, 50 (57.5%), of all respondents. There were 37 (42.5%) female respondents.

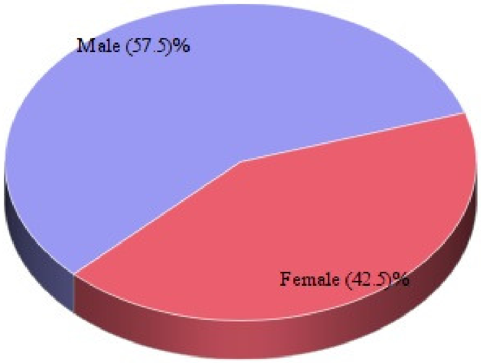

Fig. 2. Participants' gender profile.

Looking at the age profile of the participants, we found that those over the age of 40 represent the largest percentage of the total number of respondents .Out of 87 respondents, 32 (36.8%) were above 40.The second largest group comprised those between the ages of 31-35, which totalled 25 (28.7%) respondents. The age group 36-40 had 23(26.4%) responses, while the age group 26-30 contributed only 7 (8%) respondents. There were no participants age 25 or younger. Fig. 3 shows the participants' age profile.

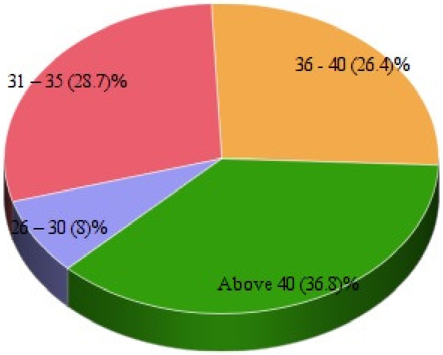

Fig. 3. Participants' age profile.

Fig. 4 shows the positions held by respondents in their organizations. This figure shows that the bulk of participants, 25 (28.7%) were specialists. The employee group was the second largest, 21 (24.1%), and the technician group was the third largest, 18 (20.7).The smallest groups were the chief-employee, management and other groups, with less than 10 respondents for each, 10.3%, 6.9% and 9.2%, respectively.

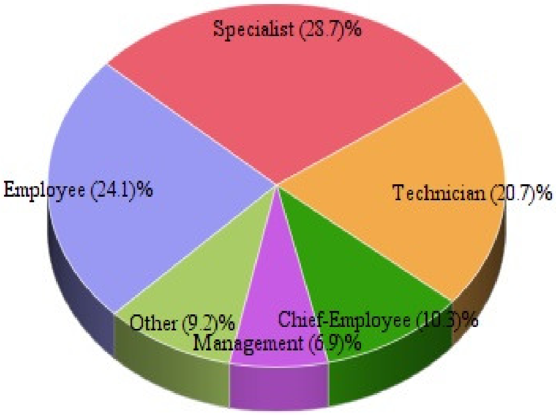

Fig. 4. Participants' position profile.

The work experience profile contained four sets, as shown in Fig. 5. Employees with more than 10years of work experience represented the largest number of respondents in this study, 59 (67.8%). Those with 6-10 years of work experience comprised the second largest group, 22 respondents (25.3%). Finally, the last groups, those with work experience of 1-2 and 3-5 years, had an equal number of respondents, 3 (3.4%).

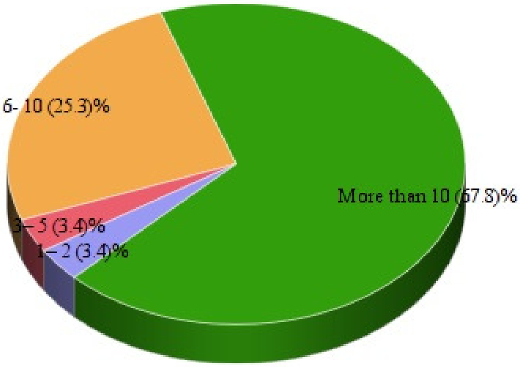

Fig. 5. Participants' work experience profile.

Fig. 6 represents the level of education of the participants. Five segments were determined for the participants' qualifications profile: diploma or less, high diploma, bachelor's, master's, and PhD. The largest number of participants were holders of bachelor's degrees, 48 (55.2%). Master's degree holders were the second largest group, 21 (24%), and respondents with a higher diploma were the third largest, 10 (11.5%). Finally, respondents with a diploma or lesser qualification, as well as those holding PhDs, were the lowest number of respondents. The respondents with diploma qualifications or less totalled 6 (6.9%), while only 2 (2.3%) respondents had earned PhDs.

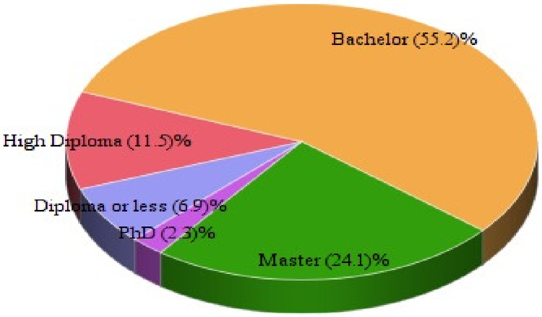

Fig. 6. Participants' education profile.

Fig. 7 shows the respondents' level of ISA profile. Because Omani public sector institutions offer continuous training and awareness sessions to their employees, the level of ISA is assessed for the trainee to determine whether his/her level is elementary, intermediate or advanced. This profile was adopted as one of the controllers. For all 87 collected responses, 53 (60.9%) respondents were at the intermediate level, 20 (23%) were at the advanced level and 14 (16.1%) were at the elementary level.

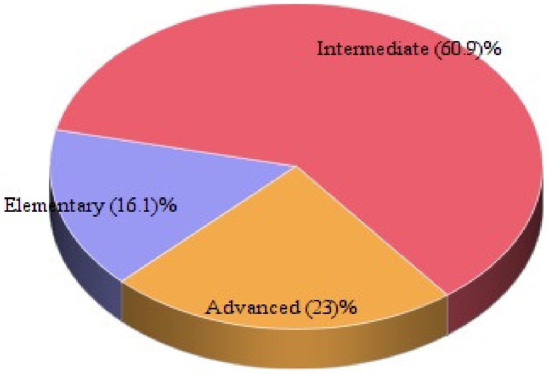

Fig. 7. Participants' level of ISA profile.

The last demographic profile was the organization to which the respondents belong. Since the study population includes all the employees of the Omani public sector institutions, these institutions were classified into four main sections. The education sector includes the Ministries of Education and Higher Education, the Institution of Public Administration, and technical colleges affiliated with the Ministry of Manpower. The health sector includes only the Ministry of Health, which employs approximately 40,000 individuals [32]. The services sector includes service ministries such as the Ministries of Civil Service, Housing, Social Development, Regional Municipalities and Water Resources. Finally, the other sector includes institutions such as the Al-raffd fund and the national museum. Figure 8 shows that 54 (62.1%) education sector employees responded, while other and service sector respondents numbered 16 (18.4%) and 15 (17.2%), respectively. The health sector supplied the fewest responses, 2 (2.3%).

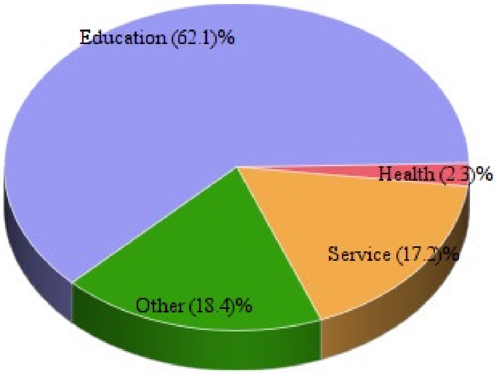

Fig. 8. Participants' organization profile.

VII. INSTRUMENT RELIABILITY RESULTS

In this pilot study, Cronbach's alpha test, the most common method of measuring internal consistency and testing the study's questionnaire reliability, was used [37]. Cronbach's alpha values range from 0 to 1; usually the agreed minimum for accepting reliability is 0.7 [38].All loading values of this study were above 0.70, which indicates good questionnaire reliability.

Table 4: Reliability analysis.

Factor	Code	No. of Items	Cronbach's Alpha
Attitude	ATT	6	0.912
Subjective Norms	SN	6	0.851
Perceived Behavioural Control	PBC	5	0.832
Response Efficacy	RE	5	0.766
Perceived Vulnerability	PV	5	0.795
Perceived Certainty of Sanctions	PCOS	5	0.863
Perceived Severity of Sanctions	PSOS	6	0.779
Behavioural Intention	BI	7	0.859
Actual Behaviour	AB	9	0.870
Organizational Support	OS	5	0.885
Communication	COM	5	0.870
Total of Items		**64**	**0.910**

As seen in Table 4, 10 variables had values that ranged between 0.7 to 0.899 and were thus all classified as acceptable: subjective norms (0.851), perceived behavioural control (0.832), response efficacy (0.766), perceived vulnerability (0.795), perceived certainty of sanctions (0.863), perceived severity of sanctions (0.779), behavioural intention (0.859), actual behaviour (0.870), organizational support (0.885) and communication (0.870). Furthermore, one variable demonstrated an excellent value; attitude had a value of (0.912). The Cronbach's alpha values of this study's model range from 0.766 to 0.912; therefore, all the reliabilities are deemed acceptable and ready to be used for the main survey. Note that these results are true for Omani public sector only.

VIII. RESULTS OF VARIABLES' RELATIONSHIP

The correlations values between two variables ranges of (+1) to (-1) where the value of +1 refers to total perfect correlation. The value of -1 refers to a perfect total negative correlation, while the value of 0 refers to no linear correlation or the absence of a relationship [39]. The correlation results of this study show that attitude (r = .241*, $p < 0.05$), subjective norm (r = .284**, $p < 0.01$), perceived behavioural control (r = .360**, $p < 0.01$), response efficacy (r = .334**, $p < 0.01$), perceived vulnerability (r = .290**, $p < 0.01$), perceived certainty of sanctions (r = .266*, $p < 0.05$) and perceived severity of sanctions (r = .242*, $p < 0.05$) are positively and significantly associated with behavioural intention towards employees' ISA actual behaviour. Furthermore, the correlation findings indicate that organizational support (r = .342**, $p < 0.01$) and communication (r = .426, $p < 0.01$) are positively and significantly associated with employees' ISA actual behaviour. Finally, behavioural intention (r = .505**, $p < 0.01$) is positively and significantly associated with employees' ISA actual behaviour. Table 5 presents the correlations among the variables for this study.

The results of this study confirm the existence of the relationships between employees' ISA behavioural intention and actual behaviour on the one hand and between the chosen variables on the other. Hence, the findings contribute to the body of ISA literature in general and in Oman especially, noting that these results are true in Omani society only.

Table 5: Pearson correlation coefficient among the variables.

		ATT	SN	PBC	RE	PV	PCOS	PSOS	OS	COM	AB
BI	Pearson Correlation	.241*	.284**	.360**	.334**	.290**	.266*	.242*	-	-	.505**
	Sig. (2-tailed)	.024	.008	.001	.002	.007	.013	.024			.000
	N	87	87	87	87	87	87	87	87	87	87
AB	Pearson Correlation	-	-	-	-	-	-	-	.342**	.426**	-
	Sig. (2-tailed	-	-	-	-	-	-	-	.001	.000	-
	N	87	87	87	87	87	87	87	87	87	-

**. Correlation is significant at the 0.05 level (2-tailed).*

***. Correlation is significant at the 0.01 level (2-tailed).*

IX. DISCUSSION ON RESULTS

To determine the reliability of the questionnaire scale for the collected data of this pilot study [31, 36], SPSS Statistics 23 software was used. The instrument (self-administered questionnaire) used in this pilot study has achieved a high degree of validity and reliability. This means that, the questionnaire has the potential to improve the accuracy and reliability of the results that will be obtained later. The descriptive analysis indicates that skewness values show an almost normal distribution [36, 40]. All questionnaire items of utilized variables were above 0.70, which indicates good questionnaire reliability [37, 38], therefore, all the reliabilities are deemed acceptable and ready to be used for the main survey based on the results of Cronbach's alpha test. Furthermore, we conclude by Pearson correlation analysis test [39], that the findings assure the existence of the relationships between utilized dependant and independent variables.

X. CONCLUSION

This pilot study has been conducted to overcome the problem of a lack and imbalance of ISA among Omani public sector employees. The proposed model of the study depended on integrating three psychological theories, the theory of planned behaviour (TPB), protection motivation theory (PMT) and general deterrence theory (GDT), in addition to two facilitating conditions variables, organizational support and communication, in order to present a new conceptual model for enhancing ISA in Oman. All items of the variables utilized in the proposed model have been shown to be reliable with acceptable and excellent values of Cronbach's alpha.

The study makes a substantial theoretical contribution to the body of ISA knowledge about how to employ successful factors for the control, prediction, motivation and deterrence that direct employees' compliance for both behavioural intention and actual behaviour towards IS policy. To the best of our knowledge, this is the first study that depends on a combination of control, prediction, motivation and deterrence factors and provides theoretical, exploratory and empirical support for the results of behavioural intent and actual behaviour together to comply with information security policies for Omani public sector employees. This research has the limitation that the results are only applicable to Omani society and possibly to neighbouring countries that share a similar culture.

XI. FUTURE SCOPE

Future work will be to use the findings of this study to conduct a major survey to investigate the enhancement of ISA in Oman, but with a larger sample size in excess of 400 respondents.

ACKNOWLEDGMENTS

The authors of the paper would like to acknowledge the assistance of Dr. Nabil Hussein Alfahim at IIUM University, Malaysia in conducting statistical methods. Moreover, the authors are grateful to the employees of Omani public sector for their response to this pilot study. The primary author would like also to extend his unending gratitude to Dr. Warusia Yassin co author for his supervision for this study and to the University Teknikal Malaysia Melaka (UTeM), CyberSecurity Malaysia and INSFORNET research group for their supports in this study.

Conflict of Interest. There is no conflict of interest for any of the authors regarding the publication of this paper.

APPENDIX A: Constructs and items

Attitude	ATT1	Information security awareness is necessary.
	ATT2	Information security awareness is beneficial.
	ATT3	Practicing information security awareness is useful.
	ATT4	I believe that information security awareness is a useful behavioral tool to safeguard the organization's information assets.
	ATT5	My information security awareness has a positive effect on mitigating the risk of information security breaches.
	ATT6	Information security awareness is a wise approach that decreases the risk of information security incidents.
Subjective Norms	SN1	Information security awareness culture in my organization influences my behavioral intention.
	SN2	My colleagues think that I should have information security awareness to protect organizational information assets.
	SN3	My friends in my office encourage me to understand information security policies
	SN4	The head of department thinks that information security awareness is a value culture.
	SN5	The head of department believes that I should be aware on how to protect organizational information assets.
	SN6	The senior staff in my organization have a positive view on information security awareness.
Perceived Behavioral Control	PBC1	Information security awareness is an achievable practice.
	PBC2	I have the necessary awareness about information security to share with the other employees.
	PBC3	I have the ability to adopt information security awareness to mitigate the risk of information security breaches.
	PBC4	Information security awareness adoption is an easy and enjoyable task for me.
	PBC5	I have enough knowledge to behave safe in terms of information security.
Response Efficacy	RE1	Enabling the security measures on my work computer is an effective way to deter hacker attacks.
	RE2	Enabling security measures at my workplace will prevent hackers from gaining access to important personal or financial information.
	RE3	At my work, efforts to ensure the safety of my confidential information are effective
	RE4	The preventative measures available to me to stop people from gaining access to my organization’s information are adequate
	RE5	The preventative measures available to me to prevent people from damaging my information system at work are adequate
Perceived Vulnerability	PV1	I know my organization could be vulnerable to security breaches if I don’t adhere to its information security policy.
	PV2	I could fall victim to a malicious attack if I fail to comply with my organization’s information security policy.
	PV3	I believe that trying to protect my organization’s information will reduce illegal access to it.
	PV4	My organization’s data and resources may be compromised if I don’t pay adequate attention to guidelines.
	PV5	Information security breaches are becoming more and more serious.
Perceived Certainty of Sanctions	PCOS1	Employee computer practices are properly monitored for policy violations.
	PCOS2	I believe that if I violate confidentiality of information the management will realize it.
	PCOS3	If I violate organization security policies, I would probably be caught.
	PCOS4	I believe that if I transfer organizational information outside the organization will find out my violation.
	PCOS5	I believe that if I sell organizational information my organization will discover it.
Perceived Severity of Sanctions	PSOS1	The organization disciplines employees who break information security policies.
	PSOS2	My organization terminates employees who repeatedly break information security policies.
	PSOS3	If I was caught violating my organization’s information security policies, I would be severely punished.
	PSOS4	I deserve punishment if I violate the confidentiality of organizational information
	PSOS5	I think punishment will be high if I sell or transfer organizational information

		outside.
	PSOS6	I think receiving sanctions because of my information security misconduct will negatively influence my career development.
Behavioural Intentions	BI1	I am willing to practice my information security awareness because of its potential to reduce the risks.
	BI2	I will share my information security awareness with my colleagues to comply with security policies.
	BI3	I intend to help my colleagues to increase their awareness of information security.
	BI4	I intend to collaborate with other staff to decrease insider threats in my organization.
	BI5	I will inform the other staff about new methods and software that can reduce the risk of information security.
	BI6	I will share the report on information security incidents with others, in order to reduce the risk.
	BI7	I plan to have safe information security behaviour.
Actual Behavior	AB1	I frequently practice my experience about information security with my colleagues.
	AB2	I practice my information security knowledge with my colleagues.
	AB3	I frequently share my expertise from my information security training with my colleagues.
	AB4	I frequently talk with others about information security incidents and their solutions in our meetings.
	AB5	I avoid mistakes in the domain of information security.
	AB6	I always mitigate information security threats.
	AB7	I think about the consequences of my behaviour before any action.
	AB8	I am careful about my behaviour in the domain of information security.
	AB9	I frequently asses my information security behaviour to improve it
Organizational Support	OS1	Information security awareness is of value in my organization.
	OS2	The organization cares about my information security awareness level.
	OS3	The management appreciates employees for their information security awareness.
	OS4	The management awards employees for their compliance with information security policies.
	OS5	The management encourages employees to information security awareness adoption.
Communication	COM1	(in organization) We have communication channels established for employees to report information security suspected improprieties.
	COM2	The management communicates employees' security duties and control responsibilities in an effective manner.
	COM3	Communication flows across the organization adequately (e.g. from department to department) to enable employees to discharge their responsibilities in an efficient security.
	COM4	I feel as though I am a part of the information security decision-making process within my organization.
	COM5	The relationship I have with my superiors makes it easy to talk to them whenever there is an information security problem.

REFERENCES

[1]. Jing, F., & Pengzhu, Z. (2009). A field study of G2G information sharing in Chinese context based on the layered behavioral model. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1-13). IEEE.

[2]. Fan, J., & Zhang, P. (2011). Study on e-government information misuse based on General Deterrence Theory. In *ICSSSM11* (pp. 1-6). IEEE.

[3]. Bharathi, S., & Suguna, J. (2014). A Conceptual Model To Understand Information Security Awareness. *International Journal of Engineering.*

[4]. Safa, N., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57,* 442-451.

[5]. Khan, B., Alghathbar, K., Nabi, S., & Khan, M. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, Vol. *5*(26), 10862.

[6]. Al-Shanfari I, Yassin W, Abdullah R. (2020). Identify of Factors Affecting Information Security Awareness and Weight Analysis Process. *International Journal of Engineering and Advanced Technology (IJEAT)*. Vol. *9*(3): 534-42.

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

[8]. Alshanfari, I., Ismail, R., Zaizi, N, & Wahid, F. (2020). Ontology-based Formal Specifications for Social Engineering. *International Journal of Technology Management and Information System,* Vol. 2*(*1), 35-46.

[9]. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and

behavior: a theory-based literature review. *Management Research Review*, Vol. 37(12):1049-92.

[10]. Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer,* Vol. *43*(2), 64-71.

[11]. Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

[12]. Fishbein, M., & Ajzen, I. (1981). On construct validity: A critique of Miniard and Cohen's paper. *Journal of Experimental Social Psychology,* Vol. *17*(3), 340-350.

[13]. Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security,* Vol. *53,* 65-78.

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

[15]. Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior,* Vol. *28*(5), 1849-1858.

[16]. Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 94-102).

[17]. Rogers, R. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

[18]. Gundu, T., & Flowerday, S. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal,* Vol. *104*(2), 69-79.

[19]. Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management,* Vol. *33*(1), 2-16.

[20]. Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security,* Vol. *79*, 68-79.

[21]. Stafford, M. C. (2015). Deterrence Theory: Crime. *International Encyclopedia of the Social & Behavioral Sciences, 255–259*.

[22]. Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management,* Vol. *49*(2), 99-110.

[23]. D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* Vol. *20*(6), 643-658.

[24]. Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security,* Vol. *39,* 447-459.

[25]. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, Vol. *37,* 1049–1092.

[26]. Triandis, H. (1979). Values, attitudes, and interpersonal behavior. In *Nebraska symposium on motivation*. Belief, attitudes, and values (pp. 195–259).

[27]. Jeon, S., Kim, Y., & Koh, J. (2011). Individual, social, and organizational contexts for active knowledge sharing in communities of practice. *Expert Systems with applications,* Vol. *38*(10), 12423-12431.

[28]. Stewart, G. (2009). A safety approach to information security communications. *Information security technical report,* Vol. *14*(4), 197-201.

[29]. Stewart, G., & Lacey, D. (2012). Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security,* Vol. *20*(1), 29-38.

[30]. Bada, M., & Sasse, A. (2018). Cyber security awareness campaigns: Why do they fail to change behaviour? 2014. *Global Cyber Security Capacity Centre, University of Oxford, Retrieved*, 24.

[31]. Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

[32]. MOCS (2018). The annual statistics of civil service employees. Ministry of Civil Service. http://portal.mocs.gov.om/pdf_files/stat2017.pdf Accessed April 30, 2020.

[33]. Safa, N., Maple, C., Furnell, S., Azad, M., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems,* Vol. *97*, 587-597.

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

[25]. Peace, A., Galletta, D., & Thong, J. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems,* Vol. 20(1), 153-177.

[36]. Hair, J., Ringle, C., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long range planning,* Vol. *46*(1-2), 1-12.

[37]. Cronbach, L. (1947). Test "reliability": Its meaning and determination. *Psychometrika,* Vol. *12(*1), 1-16.

[38]. Nunnally, J. and Bernstein, I. (1994). The reliability of Reliability. Psychometric Theory. 3rd ed. New York. McGraw-Hill, 1994.

[39]. Adler, J., & Parmryd, I. (2010). Quantifying colocalization by correlation: the Pearson correlation coefficient is superior to the Mander's overlap coefficient. *Cytometry Part A,* Vol. *77*(8), 733-742.

[40]. Holmes, W., & Rinaman, W. (2014). Describing the Distribution of a Quantitative Variable. In *Statistical Literacy for Clinical Practitioners* (pp. 87-125). Springer, Cham.

How to cite this article: Al-Shanfari, I., Yassin, W., Abdullah, R. S. and Magrisi, G. (2020). Enhancing Information Security Awareness among Omani Public Sector Employees: A Pilot Study. *International Journal on Emerging Technologies*, *11*(3): 1194–1203.