Journal of Theoretical and Applied Information Technology
30th June 2021. Vol.99. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTRODUCING A NOVEL INTEGRATED MODEL FOR THE ADOPTION OF INFORMATION SECURITY AWARENESS THROUGH CONTROL, PREDICTION, MOTIVATION, AND DETERRENCE FACTORS: A PILOT STUDY

[1]ISSAM AL-SHANFARI, [*]WARUSIA YASSIN, [2]RAIHANA SYAHIRAH ABDULLAH, [3]NABIL HUSSEIN AL-FAHIM, [4]ROESNITA ISMAIL

[* and 2] Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, MALAYSIA
[1]Information Technology Department, Ministry of Education, Salalah, OMAN
[3]Business Administration, KICT, International Islamic University Malaysia, MALAYSIA
[4]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Negeri Sembilan, MALAYSIA
E-mail: [*] s.m.warusia@utem.edu.my, [1] issam.malqoot@moe.om

ABSTRACT

Information security (IS) violations have a negative impact at both organisational and individual levels. Information security awareness (ISA) therefore plays a positive role in ensuring employees adhere to an organisation's security policies. The challenges that arise in protecting the information infrastructure in the Omani public sector are increasing because of a rise in cases of piracy and phishing attempts as well as a lack of adequate ISA among employees. This paper discusses a pilot study from our ongoing research that proposes an integrated model for adopting ISA as an effective method to improve the security behaviour of employees in Omani institutions. This study aims to validate the reliability of research instrument items prior to conducting a main survey on the adoption of the ISA model in Oman. PLS-SEM and SPSS software were used to conduct statistical analyses, which included a skewness test, a correlation analysis, a Cronbach's alpha test, and tests for composite reliability (CR), average variance extracted (AVE), and discriminant validity. Three main theories were utilised in the formation of the integrated ISA model: the theory of planned behaviour (TPB), protection motivation theory (PMT), and general deterrence theory (GDT) – along with two facilitating condition-related constructs: organisational support and communication. The findings indicated that all construct items for all variables have acceptable Cronbach's alpha values, composites reliability, AVE, and discriminant validity. The results of this study reveal that the questions were applicable, subject to one interpretation, to all participants. Hence, this study contributes to the body of ISA literature by discussing ISA in terms of the bases of control, prediction, motivation, and deterrence. This synthesis constitutes a new perspective that enables organisations to better manage the ISA process, particularly in Oman.

Keywords: *Enhancing security awareness, Information security awareness, Pilot study, PLS-SEM, Survey.*

1. INTRODUCTION

One of the main challenges encountered by organisations and firms is how to maintain the confidentiality of information and its infrastructure, as these information assets are a vitally important competitive resource [1]. Inaction and lack of seriousness in protecting an institution's sensitive information can have serious consequences, including the loss of intellectual property, damage to the institution's reputation, and a reduced competitive advantage [2]. Information leakage refers to the intentional or unintentional transfer of information to other parties unauthorised to receive it [3]. Technical measures alone cannot provide an absolutely safe environment for information assets, and security measures cannot be effective without sufficient awareness among staff of what needs to be done [4]. Therefore, it is essential to focus on education and to be aware of the human element, which must be achieved in parallel with an investment in technical methods to protect information. The activation of managerial aspects by the institution is necessary for the protection and

integrity of information. Some studies have indicated that internal users may be both the problem and the solution to implementing security policies within an organisation [4], [8], [46]. Numerous studies recommend increasing the attention paid to the human element [5], [6], [7] to mitigate or reduce security breaches. In continuation of our previous work which identified the factors that influence ISA when adopting awareness campaigns [4], the current research aims to raise security awareness among Omani public sector employees by introducing a new model based on prediction, control, motivation, and deterrence factors. The dependent variable was actual behaviour, and the mediator variable was behavioural intention. The independent variables were nine variables that have not previously been examined in a collective manner in the ISA literature. Research in developing Arab countries on enhancing ISA, particularly in Oman, is currently lacking. Hence, the primary purpose of this paper is to conduct a pilot study to validate questionnaire items for the proposed model of enhancing ISA in Oman, prior to conducting the main survey with employees working in various units of the Omani public sector.

The theoretical background to the study, along with descriptions of relevant psychological theories and facilitating conditions, is presented in the next section. Gaps in the related literature are then justified in section three, which is followed by a description of the methodology in section four. In the fifth section, the results of the statistical analyses (descriptive statistics, reliability and validity tests, and relationships between variables) are presented and discussed. Finally, a conclusion – along with a discussion of limitations and potential future work – is presented in section six.

2. THEORETICAL BACKGROUND

Based on the factors of prediction, control, motivation, and deterrence, we incorporated several factors from three different psychological theories along with two facilitating conditions in a model designed to raise ISA among employees and maintain the information infrastructure of organisations. The model included three constructs from TPB, two constructs from PMT, two constructs from GDT, and two facilitation conditions. It is important that the model is developed based on different perspectives as this will help to enhance the security awareness process among employees in line with security regulations. Several studies [1], [4], [5], [8], [9], [10] on information security have indicated that incorporating different theories into the development of new models improves employee perceptions and behavioural intentions.

2.1. Theory of Planned Behaviour (TPB)

TPB has been widely applied in various fields to explore human behaviour, and is an extension of the theory of reasoned action (TRA) [11], which became necessary due to limitations of TRA in dealing with behaviour over which individuals have incomplete optional or volitional control. TPB suggests that intentions are the basis of the motivation to perform behaviour as they are influenced by attitudes, subjective-norms, and perceived behavioural control [12].Attitudes refer to an individual's general feelings or personal motivations towards a behaviour. Social pressure is encapsulated by subjective norms, which area person's perception of the specific behaviour that significant others, such as managers, co-workers, and parents, want him/her to perform. Perceived behavioural control refers to the level of perceived ease or difficulty a person has in performing such behaviour [12]. TPB has exhibited good results in the IT field [2], [6], [7], [8], [13], especially in controlling employee beliefs.

2.2. Protection Motivation Theory (PMT)

Rogers [14] proposed PMT based on cognitive processing and expected value theories, which he then extended to the field of health awareness and safety [15].PMT theorises the recognition and understanding of fear appeals, where the receipt of information about potential threats by an individual creates an awareness and perception of the risks to which they may be exposed. PMT consists of threat appraisal and coping appraisal. It is considered a powerful theory that provides a clear basis for predicting behavioural intent in the adoption of preventive measures [13].Several studies [6], [7], [16], [17] have demonstrated the effectiveness of PMT in implementing compliance and adherence to security policies among employees of organisations. In this study we utilised one factor from threat appraisal constructs: perceived vulnerability, and one from coping appraisal constructs: response efficacy, because these were the factors identified as having a positive impact in the related literature.

2.3. General Deterrence Theory (GDT)

GDT was originally attributed to the philosophers Cesare Beccaria and Jeremy Bentham, as it was employed in criminology as a mechanism to reduce the extent to which people engage in deviant behaviours [18]. GDT assumes that human behaviour is somewhat rational and thus can be influenced by positive incentives inherent in rewards, especially negative incentives ingrained in formal sanctions [19]. GDT suggests that waiving or threatening to impose penalties can alter employee's decisions when the severity of the potential sanction is weighed against the potential benefit of engaging in a specific behaviour [20].Perceived certainty of sanctions and the perceived severity of sanctions are the two main constructs of GDT and both are included in the proposed research model. GDT has been successfully applied in IT and information security research [5], [21], [22], [23].

2.4. Facilitating Conditions

Facilitating conditions are factors that are added to others to enable people to perform tasks and activities easily and conveniently [24]. This study is concerned with two facilitating conditions (organisational support and communication) that influence the actual behaviour of employees in line with the information security policies of an organisation. Studies have shown that organisational support has a significant impact on knowledge sharing in the fields of technology and information security [8] as well as on communities of practice [25].With respect to communication, we contend that good communication between employees on all information security issues can address human weaknesses in acquiring sufficient awareness in line with policies and regulations [26], [27]. Thus, good communication can enable employees to gain effective skills, make good decisions, and reduce false assumptions regarding information security [28]. Figure 1 depicts the proposed study model in a concise form.

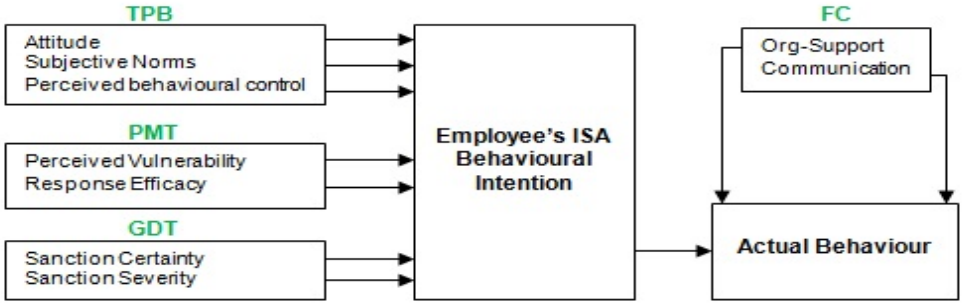

Figure 1: Study Model.

3. THE GAPS IN ISA-RELATED LITERATURE

Through our review [4] of the relevant literature, we found that most of the studies that relied on developing models for ISA focused on behavioural intentions or actual behaviour only. Therefore, focusing on both aspects together is extremely important and requires further investigation [29]. Facilitation conditions have also been largely ignored in research related to ISA; this also needs to be addressed through further investigation. To fill these gaps, this study adopted its proposed model by focusing on both behavioural intention and actual behaviour, in addition to two facilitating conditions: organisational support and communication. Current understanding will be enhanced by including these factors and verifying that they can enhance ISA by employing a combination of control, motivation, prediction, and deterrence factors –which aid the management of human consciousness from a broad perspective to achieve optimal behavioural security practices. Moreover, it must be noted that until this study was conducted, no previous studies had considered ISA in Oman from the perspective of public sector employees, nor had they considered the factors affecting the awareness-raising process and the potential relationships between them.

4. METHODOLOGY

This study strives to find an effective mechanism to manage and educate people about information security, as awareness is a highly effective approach in preventing or reducing

security breaches that expose information to unauthorised disclosure. The factors of prediction, motivation, control, and deterrence were envisioned in the process of adopting ISA through the utilisation of TPB, PMT, and GDT theories and the inclusion of two facilitating conditions in the proposed model. Before proceeding with the main survey, the primary objective for this paper was to validate the reliability of the questionnaire items and ensure they were appropriate and compatible with our understanding of the model. A quantitative research design was deemed most suitable for the current study. This is because it enabled us, through hypotheses testing, to statistically determine the effect of the main factors that impact the behavioural intentions of Omani public sector employees towards engaging in actual ISA behaviour. Related previous studies helped us to develop the questionnaire for this study, which contained two main sections: the first relates to the characteristics of the respondents and contains seven questions, while the second contains questions related to the constructs included in the study mode with a total of fifty-six questions for all constructs, as shown in Table 1. Participants gave their response to each item on a five-point Likert scale. The data were collected via a self-administered survey using a stratified sampling technique based on the list provided by the Ministry of Civil Services in Oman [30]. We then classified all Omani public sector institutions into four categories according to the tasks of each unit: education, health, services and "other". Of the 122 surveys that were distributed, 100 questionnaires were returned which represented an 86% response rate. The sample size of n=100 was considered sufficient for the pilot study.

Table 1: Constructs & Items.

Factor	Items	Reference
Behavioural Intentions	7	[1], [8]
Actual Behaviour	7	[1], [8]
Attitudes	4	[7], [8]
Subjective Norms	5	[1], [7], [8]
Perceived Behavioural Control	4	[1], [7], [8]
Perceived Vulnerability	4	[6], [7]
Response Efficacy	5	[6]
Perceived Certainty of Sanctions	5	[1], [31], [32]
Perceived Severity of Sanctions	5	[1], [31], [32]
Organisational Support	5	[8], [24], [25]
Communication	5	[26], [27], [28]

4.1. Demography

As stated previously, a hundred (100) questionnaires were returned and were valid for statistical analysis. As shown in Table 2, 56 (56%) of the participants were male. In terms of age, 34 (34%) were aged 31–35 and 26 (26%) were aged 36–40. In terms of role, 31 (31%) were in an 'employee' position, 27 (27%) were technicians, and 16 (16%) were in 'other' positions. Regarding years of experience, 38 (38%) of participants had more than 10 years of experience and 34 (34%) had more than 6–10 years of experience. The most common qualification held by respondents was a bachelor's degree (44; 44%), followed by a higher diploma (26; 26%). Most of the participants were at the intermediate level of ISA (50; 50%), with 38 (38%) at an advanced level. The majority of participants belonged to units classified under the categories of education (44; 44%), services (24; 24%) and other (23; 23%).

Table 2: Demographic Details of Participants.

Factors	Items	Frequency	%
Gender	Male	56	56
	Female	44	44
Age	25 or Less	10	10
	26–30	10	10
	31–35	34	34
	36–40	26	26
	Above 40	20	20
Position	Employee	31	31
	Specialist	14	14
	Technician	27	27
	Chief-Employee	10	10
	Management	2	2
	Other	16	16
Experience	1–2 years	10	10
	3–5 years	18	18
	6–10 years	34	34
	Above 10 years	38	38
Education	Diploma	15	15
	High Diploma	26	26
	Bachelor	44	44
	Master	13	13
	PhD	2	2
Level of ISA	Elementary	12	12
	Intermediate	50	50
	Advanced	38	38
Organization	Education	44	44
	Health	9	9
	Service	24	24
	Other	23	23

5. RESULTS AND DISCUSSION

This section includes descriptive statistics for the research instrument items, an assessment of their reliability and validity, and Pearson correlation tests of the relationships between variables.

5.1. Descriptive Statistics

Descriptive statistics are commonly used to summarise or describe the characteristics of a sample or a dataset under study, such as the mean, frequency, and standard deviation. This type of statistical analysis can assist others in understanding the collective characteristics of the elements of a data sample, as was the objective of the present study. As presented in Table 3, the highest mean was attitude (ATT) with 4.59 (91%), while the mean for perceived vulnerability (PV) was 4.33 (86%). This was followed by behavioural intention (BI), perceived severity of sanctions (PSOS), and actual behaviour (AB) with means of 4.28, 4.24, and 4, respectively (85%, 84% and 80%). In addition, most variables had a similar mean of between 3.94 and 3.76 (more than 3) representing more than 60%. Moreover, perceived certainty of sanctions (PCOS), subjective norms (SN), response efficacy (RE) had similar means of 3.940, 3.922 and 3.87, respectively (79%, 78%, and 77%). The overall mean was 4.059 (81%). The standard deviations (S.D) for all variables ranged from 0.388 to 0.847, which signifies considerable yet acceptable variability within the data set. Furthermore, a skewness test was conducted to check the normal state of the data. The skewness values indicated a normal distribution and were statistically significant. Skewness values ranged from −2.024 to 1.170, based on guidelines that suggested a cut-off critical value within the range of ±2.58 [37]. Table 3 presents the descriptive statistics for all variables.

Table 3: Descriptive Statistics for All Variables.

Variables	Mean	%	S.D	Skewness
Attitudes	4.5989	91	.38898	-0.25726
Subjective Norms	3.9228	78	.70303	-0.51037
Perceived Behavioural Control	3.8215	76	.73376	-0.58921
Response Efficacy	3.8704	77	.78499	-0.5684
Perceived Vulnerability	4.3306	86	.53370	-0.07883
Perceived Certainty of Sanctions	3.9402	78	.69739	-0.74688
Perceived Severity of Sanctions	4.2417	84	.58788	-0.04149
Behavioural Intentions	4.2868	85	.47683	1.170125
Actual Behaviour	4.0259	80	.58988	-0.04564
Organisational Support	3.8496	77	.73860	-1.36929
Communication	3.7688	75	.84789	-2.02479
Total	**4.0597**	**81**	**.46025**	

5.2. Reliability and Validity Tests

This study conducted two types of reliability tests: Cronbach's alpha and CR calculated using PLS-SEM. These tests measure the internal consistency of scale items [33, 34] which, in turn, measures the overall reliability of a set of items loaded on a latent variable. General recommendations state that the reliability of the instrument (Cronbach's Alpha) can be accepted when it is greater than 0.6 [33]; if it exceeds the 0.7 threshold, this indicates CR [34]. The findings indicate that the Cronbach's alpha values ranged from 0.747 to 0.903, while CR values ranged from 0.835 to 0.923. Therefore, all values were above the recommended value of 0.60. Table 4 presents the reliability (Cronbach's alpha) and CR reliability values for the constructs.

Journal of Theoretical and Applied Information Technology
30th June 2021. Vol.99. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Cronbach's Alpha and Composite Reliability (CR).

	No. of Items	Cronbach's Alpha	Composite Reliability
AB	7	0.848	0.885
ATT	4	0.747	0.835
COM	5	0.817	0.872
BI	7	0.903	0.923
OS	5	0.810	0.869
PBC	4	0.854	0.901
PCOS	5	0.832	0.883
PSOS	5	0.803	0.865
PV	4	0.803	0.871
RE	5	0.800	0.862
SN	5	0.773	0.842
Total	**56**	**0.854**	**0.895**

Convergent validity refers to the degree to which scales of the same variable theoretically should be related which, consequently, indicates whether the related variable's tests should be highly correlated [35]. It provides higher reliability than the Cronbach's alpha; this is why it is a fundamental part of assessing a measurement model. According to Hair et al. [35], convergent validity is adequate and confirmed using Smart-PLS if items load greater than 0.6 or 0.7 in exploratory research, and constructs have an AVE of at least 0.5.To achieve adequate convergent validity, Chin [36] recommended that the AVE of each latent variable should be at least 0.50. The factor loading analysis for this pilot study is presented in Figure 2 and indicates that all loadings are equal or more than 0.60. As per Hair et al. [37], an outer loading above 0.50 is considered significant and the item should remain.

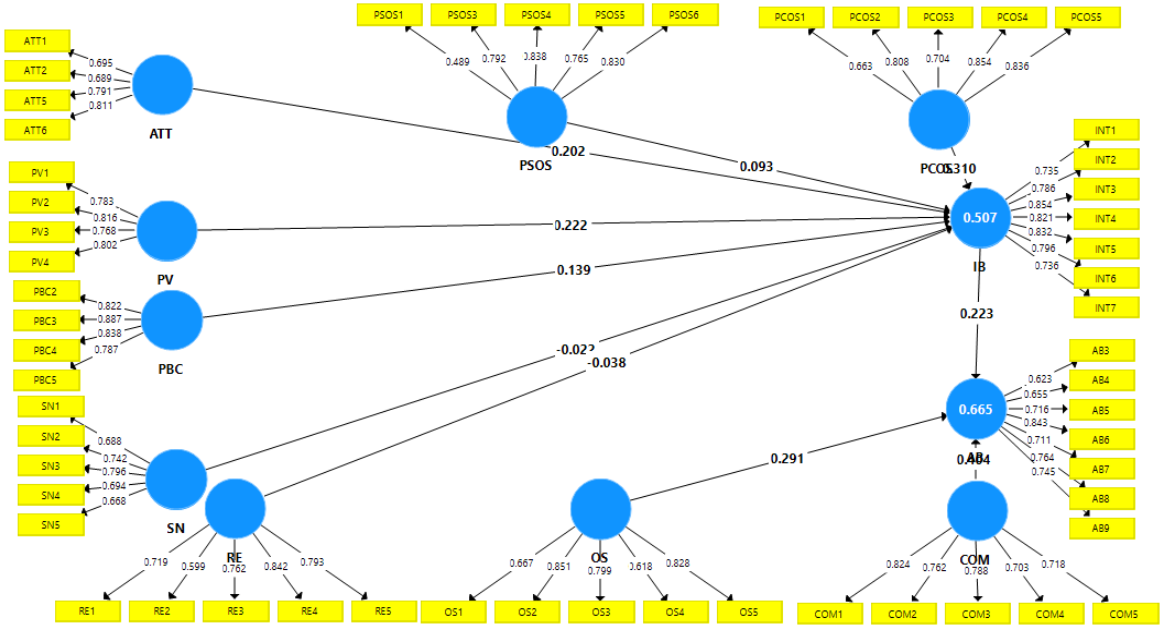

Figure 2: Measurement Model/ Outer Model

Discriminatory validity is achieved by gathering evidence to suggest that measures of latent variables that should not be correlated with one another are, theoretically, unrelated to each other [44]. The discriminatory validity is proven if the following is achieved: (1) the average variance extracted (AVE) is greater than the values in the corresponding raw and column; (2) the maximum shared squared variance (MSV) is less than the AVE; and (3) all the values in the correlation analysis table are less than 0.9[44]. In the present study, discriminant validity was indicated, as the AVE values were greater than the squared correlations for each set of constructs. In addition, the square root of the AVE for a given construct was greater than the absolute value of the correlation square of the construct with any another factor (AVE > correlation square). Table 5 presents the square root of the AVE for all constructs greater than the correlations between the construct and

other constructs in the model. These values ranged from 0.105 to 0.755. The results also indicate AVE values were greater than 0.50 and ranged from 0.517 to 0.696. Therefore, discriminant validity was supported and all constructs for this study were deemed valid.

Table 5: Discriminant Validity and AVE

	AVE	AB	ATT	COM	BI	OS	PBC	PCOS	PSOS	PV	RE	SN
AB	0.526	0.725										
ATT	0.560	0.239	0.748									
COM	0.578	0.722	0.105	0.760								
BI	0.633	0.605	0.425	0.531	0.796							
OS	0.575	0.718	0.175	0.739	0.574	0.758						
PBC	0.696	0.710	0.236	0.679	0.523	0.667	0.834					
PCOS	0.603	0.717	0.200	0.711	0.609	0.748	0.653	0.777				
PSOS	0.569	0.729	0.366	0.749	0.608	0.712	0.640	0.755	0.754			
PV	0.628	0.568	0.489	0.464	0.603	0.503	0.527	0.602	0.616	0.793		
RE	0.559	0.718	0.207	0.702	0.518	0.746	0.735	0.736	0.706	0.596	0.747	
SN	0.517	0.682	0.290	0.628	0.495	0.640	0.670	0.674	0.634	0.550	0.632	0.719

5.3. Relationships between the Variables (Pearson Correlation)

Whenever the correlation between two variables approaches the threshold of (+1), this indicates a perfect correlation, whereas when it approaches the threshold of (-1), this indicates a perfect negative correlation. Therefore, correlations between two constructs range from(+1) to (-1), with a value of 0 indicating no linear correlation [38].The correlation findings for this pilot study indicated that attitudes ($r = .244^*$, $p < 0.01$), subjective norms ($r = .770^{**}$, $p < 0.01$), perceived behavioural control ($r = .823^{**}$, $p < 0.01$), response efficacy ($r = .762^{**}$, $p < 0.01$), perceived vulnerability ($r = .544^{**}$, $p < 0.01$), perceived certainty of sanctions ($r = .775^{**}$, $p < 0.01$) and perceived severity of sanctions ($r = .757^{**}$, $p < 0.01$) were positively correlated with employees' intentions to engage in ISA behaviour. Moreover, the correlation results indicated that organisational support ($r = .769^{**}$, $p < 0.01$) and communication ($r = .790^{**}$, $p < 0.01$) were positively and significantly correlated with employees' ISA behaviour. Finally, behavioural intentions ($r = .619^{**}$, $p < 0.01$) was positively correlated with employees' ISA behaviour. Table 6 presents the correlations among the variables in the proposed model.

Table 6: Pearson Correlation Coefficients among the Model Constructs

		ATT	SN	PBC	RE	PV	PCOS	PSOS	OS	COM	AB
BI	Pearson Correlation	.244*	.770**	.823**	.762**	.544**	.775**	.757**	-	-	.619**
	Sig. (2-tailed)	.014	.000	.000	.000	.000	.000	.000			.000
	N	100	100	100	100	100	100	100	100	100	100
AB	Pearson Correlation	-	-	-	-	-	-	-	.769**	.790**	-
	Sig. (2-tailed	-	-	-	-	-	-	-	.000	.000	-
	N	100	100	100	100	100	100	100	100	100	-

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

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

The findings of this pilot study confirm the existence of relationships between the behavioural intentions of employees and their actual ISA behaviour, and between the utilised constructs. The findings contribute to enriching the body of ISA literature in general and the Omani public sector in particular, taking into account that these findings are true only in the culture of Omani society.

5.4. Discussion & Contribution

There are two important aspects to consider when conducting such a study. First, the internet is a vast and boundless environment that is impossible to control. In this environment, users' errors are increasingly exploited by hackers – which results in confidentiality violations. Information security awareness reduces user behaviours that may generate security risks. Moreover, there remains a gap between the technological aspects and the methods used in awareness of the human element, which is still somewhat traditional. The technology aspect is not the only way to ensure the security of information. Improving awareness methods so that the human component can keep pace with technological advances should also be considered. Secondly, this research is characterised by including a mixture of control, motivation, and deterrence factors, which was an outcome of combining variables of psychological theories: TPB, PMT, and GDT. These factors aim to improve employee ISA in organisations, and thus reduce information security violations and breaches. TPB is considered a useful model for predicting users' intentions towards desired actual behaviour and for controlling their beliefs, because the 'controllability' of the variable of perceived behavioural control enables individuals to control their behaviour, or their behaviour will be under the control of external forces (people who influence them) [2,8].The variables utilised from PMT aim to raise the motivation of users' intentions to adopt and use protective countermeasures; thus, this theory also provides a powerful framework for predicting a user's intention to participate in a preventive measure. Additionally, PMT relies on presenting a wide range of threat scenarios and hence offers a more holistic approach with various probabilities to maintain users' awareness [15].The constructs utilised from GDT are intended to control and alter criminal behaviour. The purpose of imposing such penalties is to impose a deterrent to reduce unwanted user behaviour. The imposition and use of penalties contribute – to some degree – to correcting the behaviours of uncooperative employees [45], and creates awareness among users and other employees of the criminal behaviour when sanctions are applied. In addition to the aforementioned factors, the proposed model was strengthened with two facilitating conditions (organisational support and communication) to facilitate actual behaviour as per the organisation's information security policies. To the best of our knowledge, this present study is one of a few focused on examining the factors of prediction, motivation, control, and deterrence collectively. It therefore forms a new perspective and provides theoretical, exploratory, and experimental support to enhance behavioural intentions and actual behavioural compliance with organisational information security policies. We believe that this work supplements the previous studies conducted in this domain.

Through the proposed model, this pilot study sought to determine the reliability [37], [39] of the research instrument (self-administrated questionnaire) for the data collected prior to conducting the main survey. Both PLS-SEM and SPSS software were utilised to determine reliability, thus ensuring the research instrument possessed a high degree of validity and reliability. This indicates that the questionnaire has the potential ability to improve the accuracy and reliability of the results that will be obtained during the main survey. The descriptive analysis indicated that the skewness values have an approximately normal distribution [37], [40].All items for utilised constructs were above 0.7, which indicates that the reliability of the questionnaire was good [41], [42]. Thence, based on the Cronbach's alpha and CR tests, the reliabilities for all items are considered acceptable. Furthermore, the findings supported the convergent validity and discriminant validity of all constructs utilised for this study. Finally, the Pearson correlation analysis [38] confirmed the existence of relationships between the variables (dependent and independent) included in the study model. Initially, from this survey of 100 respondents, we can ascertain that the way to empirically validate the utilised theories and the facilitating conditions has become a clear feature. The initial statistical analysis revealed that the factors of TPB, PMT, and GDT can be used to explain the factors underpinning ISA intentions and behaviours in Oman. This is in line with the findings of previous studies [1, 6, 7, 8, 13, 6]. The

initial statistical results and the reviewed literature demonstrate the veracity of the proposed model.

6. LIMITATIONS & FUTURE WORK

This research involved limitations. The information security policy of the organisation plays a vital role in mitigating violations and increasing employee awareness. We collected the required data from the government units for which the information security policy was established, as workers within such units are aware of the importance of information security and may better understand the concepts included in the questionnaire and the purpose of the study. Some of the 39 targeted units have not yet established an information security policy. The process of collecting data in the field of information security is not easy, even from civil units, because some units require prior permission, and this may be given but subject to investigation. Moreover, the findings of this study are only generalisable to the Omani culture and countries with a comparable culture. The results can be improved by expanding the sample to include the private and banking sectors for precision and generalisation. The results of this study will be used to conduct the main survey, which requires a sample size of more than 384 participants.

7. CONCLUSION

Rapid advancements in information technology have facilitated the implementation of organisational activities as well as improved efficiency and accuracy in work. However, a gap remains between technological advancement and an adequate level of awareness among users, which makes the protection of business secrets and organisational assets an important issue for organisations. The TPB, PMT, and GDT were used as a theoretical foundation to build the proposed study model. In this model, two directions were focused upon: behavioural intentions and actual behaviour. Behavioural intention was supported by factors utilised from psychological theories while actual behaviour was supported by the two facilitating conditions. All questionnaire items for each variable included in the proposed model were found to be reliable with acceptable values for Cronbach's alpha, CR, AVE, and discriminant validity. This study provides a theoretical and cognitive contribution to literature on how to employ control, motivation, prediction, and deterrence factors in the domain of ISA. Through this study, we sought to improve the imbalances (gaps) in the relevant literature and diversify the research on issues of information security awareness in organisations, specifically in Omani public sector units.

ACKNOWLEDGMENT

This publication has been supported by Center of Research and Innovation Management (CRIM), Universiti Teknikal Malysia Melaka (UTeM). The authors would like to thank UTeM and INSFORNET research group members for their supports.

REFERENCES

[1] Safa NS, Maple C, Furnell S, Azad MA, PereraC, Dabbagh M, Sookhak M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. Future Generation Computer Systems. 2019 Aug 1;97:587-97.

[2] Cox J. Information Systems User Security: A Structured Model of the Knowing–Doing Gap. Computers in Human Behavior. 2012 Sep 1;28(5):1849-558.

[3] Ahmad A, Bosua R, Scheepers R. Protecting organizational competitive advantage: A knowledge leakage perspective. Computers & Security. 2014 May 1;42:27-39.

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

[5] Siponen, M, Pahnila, S, Mahmood, MA. Compliance with information security policies: An empirical investigation. Computer.2010:43(2), 64-71.

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

[7] Safa, N, Sookhak, M, Von Solms, R, Furnell, S, Ghani, N, Herawan, T. Information security conscious care behaviour formation in organizations. Computers & Security.2015 Sep 1;53:65-78.

[8] Safa, N, Von Solms, R. An information security knowledge sharing model in organizations. Computers in Human Behavior.2016 Apr 1;57:442-451.

[9] Bulgurcu, B, Cavusoglu, H, Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 2010;34(3):523-548.
[10] Lebek, B, Uffen, J, Neumann, M, Hohler, B, Breitner, M. Information security awareness and behavior: a theory-based literature review. Management Research Review.2014;37(12):1049-92.
[11] Fishbein, M, Ajzen, l. Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley, 1975.
[12] Ajzen, I. The theory of planned behavior. Organizational Behavior and Human Decision Processes.1991;50(2):179-211.
[13] Gundu, T,Flowerday, S. Ignorance to awareness: Towards an information security awareness process. SAIEE Africa Research Journal. 2013;104(2):69-79.
[14] Rogers, RW. A protection motivation theory of fear appeals and attitude change. The Journal of Psychology. 1975;91(1):93-114.
[15] Rogers, R. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology: A Sourcebook. 1983;153-176.
[16] Hanus, B, Wu, Y. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. Information Systems Management.2016;33(1):2-16.
[17] Torten, R, Reaiche, C, Boyle, S. The impact of security awareness on information technology professionals' behavior. Computers & Security. 2018;79:68-79.
[18] Stafford, MC. (2015). Deterrence Theory: Crime. International Encyclopedia of the Social &Behavioral Sciences.255–259. doi:10.1016/b978-0-08-097086-8.45005-1
[19] Wenzel, M. The social side of sanctions: Personal and social norms as moderators of deterrence. Law and Human Behavior. 2004;28(5):547-567.
[20] Ugrin, JC, Pearson, JM. The effects of sanctions and stigmas on cyberloafing. Computers in Human Behavior. 2013;29(3):812-820.
[21] Gundu, T. Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. ICCWS 2019 14th International Conference on Cyber Warfare and Security. 2019 (pp. 94-102).
[22] Hovav, A, D'Arcy, J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. Information & Management. 2012;49(2):99-110.
[23] D'arcy, J,Herath, T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems. 2011:20(6):643-658.
[24] Triandis, H. Values, attitudes, and interpersonal behavior. In Nebraska symposium on motivation. Belief, attitudes, and values Lincoln, NE: University of Nebraska Press. 1975. pp. 195–259.
[25] Jeon, S, Kim, Y, Koh, J. Individual, social, and organizational contexts for active knowledge sharing in communities of practice. Expert Systems with Applications. 2011;38(10):12423-12431.
[26] Stewart, G. A safety approach to information security communications. Information Security Technical Report. 2009;14(4)197-201.
[27] Stewart, G, Lacey, D. Death by a thousand facts: Criticising the technocratic approach to information security awareness. Information Management & Computer Security. 2012;20(1):29-38.
[28] 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, 24.
[29] Han, B. User's Information Security Awareness in BYOD Programs: A Theoretical Model.Information Institute Conference, Las Vegas, NV; 2017. Accessed October7, 2020. Available from: http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_HAN.pdf.
[30] MOCS TheAnnual Statisticsof Civil ServiceEmployees. Ministry of Civil Service; 2018.Accessed April 30, 2020. Available from: http://portal.mocs.gov.om/pdf_files/stat2017.pdf.
[31] Herath, T, Rao, H. Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 2009;47(2):154-165.
[32] Peace, A, Galletta, D, Thong, J. Software piracy in the workplace: A model and empirical test. Journal of Management Information Systems. 2003;20(1):153-177.

[33] Sekaran, U. Towards a guide for novice research on research methodology: Review and proposed methods. Journal of Cases of Information Technology. 2003;8(4):24-35.
[34] Hair, JF, Black, WC, Babin, BJ, Anderson, RE, Tatham, RL. Multivariate data analysis. Vol. 5, No. 3, pp. 207-219. Upper Saddle River, NJ: Prentice hall, 1998.
[35] Hair, JF, Risher, JJ, Sarstedt, M, Ringle, CM. When to use and how to report the results of PLS-SEM. European Business Review. 2019;31(1):2-24.
[36] Chin, WW. How to write up and report PLS analyses. In Handbook of Partial Least Squares (pp. 655-690). Springer, Berlin, Heidelberg, 2010.
[37] Hair, JF, Ringle, CM, Sarstedt, M. Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. Long Range Planning. 2013;46(1-2):1-12.
[38] Adler, J., Parmryd, I. (2010). Quantifying colocalization by correlation: the Pearson correlation coefficient is superior to the Mander's overlap coefficient. Cytometry Part A,77(8), 733-742.
[39] Creswell, JW, Creswell, JD. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications, 2017.
[40] Holmes, W,Rinaman, W. Describing the Distribution of a Quantitative Variable. In Statistical Literacy for Clinical Practitioners, Springer, Cham, 2014. pp. 87-125.
[41] Cronbach, L. Test “reliability”: Its meaning and determination. Psychometrika. 1947;12(1):1-16.
[42] Nunnally, J, Bernstein, I. The Reliability of Reliability. Psychometric Theory. 3rd ed. New York: McGraw-Hill, 1994.
[43] Anderson, CL, Agarwal, R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioural intentions. MIS quarterly. 2010;34(3):613-643.
[44] Ho, R. Handbook of univariate and multivariate data analysis and interpretation with SPSS. Taylor & Francis Group, Boca Raton; 2006 Mar 24.
[45] Xue Y, Liang H, Wu L. Punishment, justice, and compliance in mandatory IT settings. Information Systems Research. 2011 Jun;22(2):400-14.
[46] Alshanfari I, Ismail R, Zaizi NJ, Wahid FA. Ontology-based Formal Specifications for Social Engineering. International Journal of Technology Management and Information System. 2020 Mar 6;2(1):35-46.

Appendix A: Constructs & Items

Attitude	ATT1	Information security awareness is necessary.	[1], [7]
	ATT2	Information security awareness is beneficial.	
	ATT3	Practicing information security awareness is useful.	
	ATT4	I believe that information security awareness is a useful behavioural tool to safeguard the organization's information assets.	
Subjective Norms	SN1	Information security awareness culture in my organization influences my behavioural intention.	[1], [7], [8]
	SN2	My friends in my office encourage me to understand information security policies	
	SN3	The head of department thinks that information security awareness is a value culture.	
	SN4	The head of department believes that I should be aware on how to protect organizational information assets.	
	SN5	The senior staff in my organization have a positive view on information security awareness.	
Perceived Behavioral Control	PBC1	I have the necessary awareness about information security to share with the other employees.	[1], [7], [8]
	PBC2	I have the ability to adopt information security awareness to mitigate the risk of information security breaches.	
	PBC3	Information security awareness adoption is an easy and enjoyable task for me.	
	PBC4	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.	[6]
	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.	[6], [7]
	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.	
Perceived Certainty of Sanctions	PCOS1	Employee computer practices are properly monitored for policy violations.	[1], [31], [32]
	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.	
	PSOS1	The organization disciplines employees who break information security policies.	[1], [31], [32]
	PSOS2	If I was caught violating my organization's information security policies, I would be severely punished.	
	PSOS3	I deserve punishment if I violate the confidentiality of	

Perceived Severity of Sanctions		organizational information	
	PSOS4	I think punishment will be high if I sell or transfer organizational information outside.	
	PSOS5	I think receiving sanctions because of my information security misconduct will negatively influence my career development.	
Behavioral Intentions	BI1	I am willing to practice my information security awareness because of its potential to reduce the risks.	[1],[8]
	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 share my expertise from my information security training with my colleagues.	[1],[8]
	AB2	I frequently talk with others about information security incidents and their solutions in our meetings.	
	AB3	I avoid mistakes in the domain of information security.	
	AB4	I always mitigate information security threats.	
	AB5	I think about the consequences of my behaviour before any action.	
	AB6	I am careful about my behaviour in the domain of information security.	
	AB7	I frequently asses my information security behaviour to improve it	
Organizational Support	OS1	Information security awareness is of value in my organization.	[1], [43], [29]
	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.	[26], [27], [28]
	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.	