Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees

Al-Shanfari I[1], Warusia Yassin[2]*, Nasser Tabook[3], Roesnita Ismail[4], Anuar Ismail[5]
Department of Computer System & Communication[1, 2]
Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, MALAYSIA[1, 2]
College of Arts and Applied Science, Computer Science Department, Dhofar University, Salalah, OMAN[3]
Faculty of Science and Technology, Universiti Sains Islam Malaysia, Negeri Sembilan, MALAYSIA[4]
Ask-Pentest Sdn Bhd, Kuala Lumpur, MALAYSIA[5]

***Abstract*—In this digital era, protecting an organisation's sensitive information system assets against cyberattacks is challenging. Globally, organisations spend heavily on information security (InfoSec) technological countermeasures. Public and private sectors often fail to secure their information assets because they depend primarily on technical solutions. Human components create the bulk of cybersecurity incidents directly or indirectly, causing many organisational information security breaches. Employees' information security awareness (ISA) is crucial to preventing poor information security behaviours. Until recently, there was little combined information on how to improve ISA and how investigated factors influencing employees' ISA levels were. This paper proposed a comprehensive theoretical model based on the Protection Motivation Theory, the Theory of Planned Behaviour, the General Deterrence Theory, and Facilitating Conditions for assessing public sector employees' ISA intentions for information security behaviour. Using a survey and the structural equation modelling (SEM) method, this research reveals that the utilised factors are positively associated with actual information security behaviour adoption, except for perceived sanction certainty. The findings suggest that the three theories and facilitating conditions provide the most influential theoretical framework for explaining public sector employees' information security adoption behaviour. These findings support previous empirical research on why employees' information on security behaviours vary. Consistent with earlier research, these psychological factors are just as critical as facilitating conditions in ensuring more significant behavioural intention to engage in ISA activities, ensuring information security behaviour. The study recommends that public-sector organisations invest in their employees' applied information security training.**

***Keywords*—Information security awareness; behaviour strategies; self-administered questionnaire; structural equation modelling (SEM)**

I. INTRODUCTION

Securing information system assets has become a primary issue for organisations in today's digital environment to protect them from criminal assaults. In recent years, both cybercrime and data breaches have expanded considerably. By 2021, cyber-crime is predicted to cost more than $6 trillion, up from $3 trillion in 2015, according to the Cybersecurity Business Report [1]. As a result, organisations are constantly struggling to protect the security of their information assets, which causes them to spend heavily on technical countermeasures [2]. However, concentrating just on the technological areas of information security is insufficient since information security is multidisciplinary, with the human factor playing a significant role. The exploitation of human factors is responsible for a considerable percentage of organisational information security incidents [1]. In other respects, human error is directly or indirectly primarily the result of security breaches, including both intentional and unintentional negative behaviour [3]. According to ENISA [4], about 77% of data breaches occur due to human vulnerability. Additionally, it has been previously shown that over half of all information security breaches are caused by staff's insufficient compliance with information security policies [5].

In consideration of this context, staff members' information security awareness (ISA) has a significant influence on their information security behaviours and their compliance with security policies [6], [7]. Previous research has asserted that a lack of staff ISA as defined by information security policies (ISP) and procedures is the main reason for sensitive information misbehaviour [3]. Additionally, ISA has been a critical concern in research and practice [8] because humans are often identified as a weak link in efforts to protect systems and networks [9]. For this reason, among others, the most recent Cyber Security Breaches Survey 2019 demonstrates that cyber security is a top priority for senior management in the workplace [10].

Even though research and practice prioritise employees' information security awareness, most employees are unaware of information security risks and challenges [6]. For instance, about 90% of cybersecurity experts reported that the organisations for which they work feel exposed to insider threats [3]. According to Jaeger [11], research on ISA is still in its infancy, with numerous new areas to be explored. Even though many studies have been done on ISA, there is still no complete picture of the concept of ISA and how it fits into other constructs [11]. Other studies support this, suggesting that ISA campaigns and education fail to influence employees' behaviour for various reasons [12], [13].

*Corresponding Author.

It has been revealed that organisations fail with their ISA campaigns because they do not appropriately employ the factors impacting personnel's ISA levels while producing the content and developing material for the ISA campaigns [13], [1]. Most importantly, it was found that there were no good ways to make exciting and valuable materials for improving ISA. As a result, several behavioural factors, such as communication channels [14, 15], were not considered when ISA campaigns or initiatives were made to keep improving ISA levels [13].

Our assessment [67] of the relevant literature revealed that most research that relied on constructing models for ISA focused only on behavioural intentions or actual behaviour. Therefore, concentrating on both aspects is crucial and needs additional research [47], [51]. In ISA-related research, facilitating conditions factors have been mostly neglected; this issue also needs thorough investigation. This research implemented its developed model by concentrating on behavioural intention and actual behaviour and two facilitating conditions: organisational support and communication channels to fill these gaps. Incorporating these factors and verifying that they can enhance ISA by employing a combination of control, motivation, prediction, deterrence, and technical-related factors—which aid in managing human thought from a broad perspective to achieve optimal behavioural security practices—will enhance the current understanding.

This study, however, is a continuation of our prior research [16], which seeks to improve ISA among public-sector organisation staff by merging motivational, control/prediction, and deterrence variables into employees' behaviour to promote security awareness and reduce breaches. This study looks at the development and evaluation of a conceptual framework based on factors from the literature on information security from previous international studies. According to the model's constructs, the mediator variable is ISA's behavioural intention, and the dependent variable is InfoSec's actual behaviour. In contrast, the independent variables are a set of ten variables that have never been investigated together in the InfoSec literature. The theoretical background and conceptual model are described in Section II, followed by the methodology and results in Sections III and IV, respectively. Section V discusses the comparative evaluation of the study model. Finally, in Section VI, the conclusion is provided, along with limitations and suggestions for future studies.

II. Theoretical Background and Conceptual Model

This study highlights a new perspective relying on protection motivation theory (PMT), theory of planned behaviour (TPB), and general deterrence theory (GDT), as well as the facilitating conditions to enhance employees' ISA intentions. The different perspectives of these theories and the facilitating conditions show the whole chain of the InfoSec behaviour adoption process. Thus, it helps organisations reduce information security breaches by changing employees' behaviour to match information security policies and rules [7, 15, 17–22]. An assessment of theories utilised in related work revealed that the theories of TPB, PMT, and GDT are most often used [23]; [24]. TBP is one of the most influential theories describing human behaviour in different fields, such as organisational behaviour, public relations, healthcare, or advertising [11]. PMT is one of the most effective models for predicting a person's motivation and intention to take preventative measures [25]. GDT provides a practical focal point for describing misbehaviour [15]. The security education, training, and awareness (SETA) initiatives are the methods through which organisations raise information security awareness, educate staff on the necessity of ISA, and train end-users to take on information security activities [26]. Furthermore, facilitating conditions help employees accomplish their duties and responsibilities more quickly and effortlessly [22]. Fig. 1 presents the study model and utilised factors in a concise form.

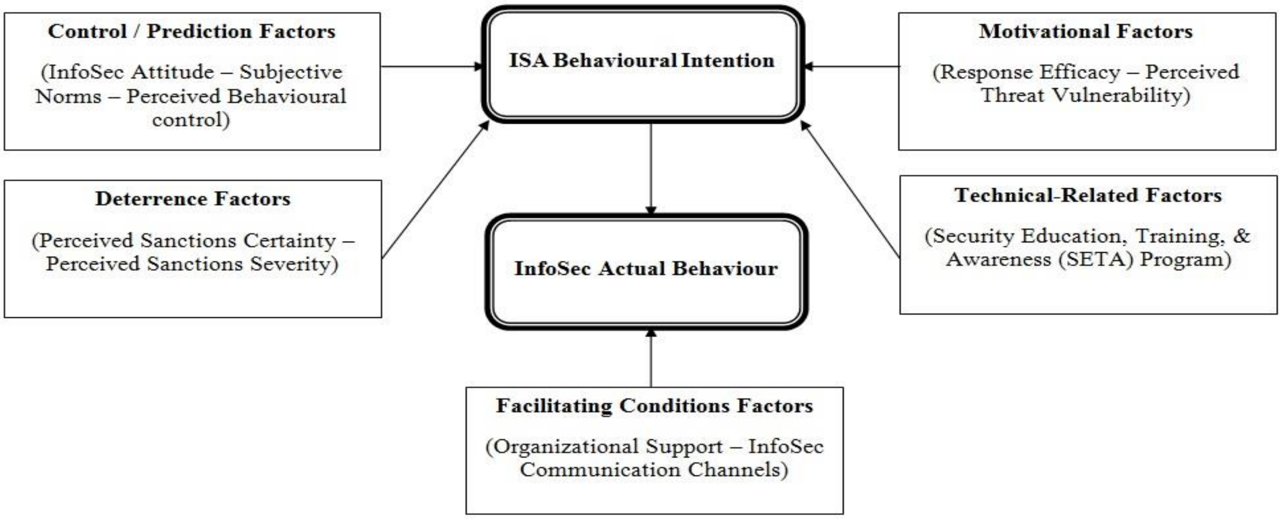
Control / Prediction Factors
(InfoSec Attitude – Subjective Norms – Perceived Behavioural control)
ISA Behavioural Intention
Motivational Factors
(Response Efficacy – Perceived Threat Vulnerability)
Deterrence Factors
(Perceived Sanctions Certainty – Perceived Sanctions Severity)
InfoSec Actual Behaviour
Technical-Related Factors
(Security Education, Training, & Awareness (SETA) Program)
Facilitating Conditions Factors
(Organizational Support – InfoSec Communication Channels)

Fig. 1. Research Model.

A. Control and Prediction Factors

Many previous studies extracted prediction and control factors from TPB theory, and its constructs were employed in the field of information technology, proving their effectiveness by controlling employees' beliefs [3], [18], [27], [28]. According to Ong and Chong [29], some researchers have benefited from more helpful and practical recommendations due to citing TPB. Additionally, some studies [30-33] have applied the TPB to predict ISP compliance, information security awareness, and knowledge sharing from an individual's behavioural perspective, making the TPB more applicable to describing how employees participate in ISA activities. Hence, avoiding and mitigating information security breaches. Commonly, human interactions influence a person's beliefs and emotions, thoughts, feelings, behaviours, and actions. TPB contends that attitudes, subjective norms, and perceived behavioural control all impact intentions, which are the foundation of motivation to do behaviour [34]. Several studies have explored the association between attitude and intention [18], [28]. Attitude determines intention, according to TPB [34]. The study intends to utilise InfoSec attitude to represent an individual's acceptance or rejection of an idea. Thus, the employee's positive InfoSec attitude towards ISA reflects his/her intention. Conversely, negative InfoSec attitudes will reduce his/her intention. Consequently, an employee who positively believes in ISA is willing to engage in ISA activities and vice versa. Thus, it is hypothesised that:

H1: Employees' InfoSec attitudes toward ISA have a positive impact on their intention to participate in ISA activities.

Subjective norms are the perceived societal constraints exerted on a person to engage in or abstain from a specific behaviour [32]. Under this social pressure, a person acquires a set of norms, values, beliefs, and motives from significant individuals such as executives, managers, and co-workers [35]. When vital individuals exercise positive pressure on the employee in the context of ISA, this positively impacts the employee's intentions [33]. Thus, it is hypothesised that:

H2: Subjective norms towards ISA engagement positively affect employees' behavioural intentions.

Perceived behavioural control is a critical component of TPB [3], which refers to an individual's sense of how easy or difficult a task or action is to accomplish. Research in the information security arena has shown that perceived behavioural control has a significant effect on behavioural intentions [15], [28], [33]. In the current study, perceived behavioural control refers to the perception that adopting information security awareness is not difficult and has a positive impact. Thus, it is hypothesised that:

H3: Perceived behavioural control towards ISA has a positive impact on the behavioural intentions of employees.

B. Motivational Factors

According to the relevant literature, the PMT model is considered one of the best theories for predicting and motivating a person's intention to take preventive steps [17], [36]. The PMT theory was developed by Rogers [37] to understand fear appeals and predict suitable responses for personal protection when faced with a threat. When a person learns about potential threats, he or she becomes more aware of the risks to which he or she may be exposed. Threat appraisal and a coping appraisal are two primary constructs in PMT. The act of determining the intensity and sensitivity of danger is referred to as threat appraisal. While evaluating the success of protective measures and the perceived self-efficacy of the person under threat is referred to as coping appraisal. Empirical studies [2], [7], [14], [38] have shown the efficacy of PMT in implementing adherence and compliance to security standards and policies among an organisation's employees. Because these were the components found to have a positive influence in the literature related to the topic, this study used one factor from threat appraisal constructs: perceived vulnerability, and one from coping appraisal constructs: response efficacy. The perceived vulnerability relates to a person's appraisal of a potentially harmful circumstance and whether or not he or she is at risk [17]. Employees who perceive a high level of vulnerability in their organisation's information systems are more likely to take preventative measures. According to previous study findings [38], employees' perceived vulnerability in a cyber-attack incident encourages them to engage in preventive measures. As a result, it stands to reason that people who believe they are not vulnerable to security risks lack appropriate security knowledge and often fail to comply with workplace security policies. On the other hand, people who believe they are more exposed to security risks are more likely to engage in ISA activities and participate in preventative activities [39]. Thus, it is hypothesised that:

H4: Perceived vulnerability toward ISA has a positive impact on the behavioural intentions of employees.

Response efficacy relates to an individual's belief that adopting or implementing a certain preventative measure is the best method to reduce security risks [40]. When a person is persuaded of the utility of a risk-reduction mechanism, he or she will almost certainly adopt risk-reduction behaviour. However, if the person is not persuaded, he or she will not adopt it [17], [36], [41]. As a result, if employees think ISA gives them enough information and awareness to keep information security breaches and risks from happening, they are more likely to be motivated to participate in ISA activities. Thus, it is hypothesised that:

H5: Response efficacy towards ISA has a positive impact on the behavioural intentions of employees.

C. Deterrence Factors

The earliest version of the deterrence theory was created by the philosophers Cesare Beccaria and Jeremy Bentham, based on the assumption that individuals seek to maximise pleasant outcomes, such as rewards, and avoid painful ones, such as penalties [42]. GDT has been chiefly used in criminology to minimise deviant behaviour in people. In recent decades, it has been successfully and efficiently used for information technology as well as preventative information security [15], [19], [20], [27], [43]. In GDT, the deterrence model is built on three core constructs: certainty of sanctions, the severity of sanctions, and celerity of sanctions. Such determinants impact people's attitudes toward preventing activities that are regarded as undesirable in society. The constructs' of GDT: perceived certainty of sanctions and perceived severity of sanctions are included in the study model due to their positive influence in the relevant literature [20], [43]. Perceived certainty of sanctions refers to a person's belief that the authorities are likely to detect delinquent behaviour. In contrast, the perceived severity of sanctions refers to the person's belief that s/he would be punished seriously if deviant behaviour is proven [3], [45]. When employees who break information security policies understand the consequences of their actions, they are more likely to participate in ISA activities and thus change their behaviour. Thus, it is hypothesised that:

H6: Perceived certainty of sanctions towards ISA has a positive impact on the behavioural intentions of employees.

H7: Perceived severity of sanctions towards ISA has a positive impact on the behavioural intentions of employees.

D. Technical-related Factors

Previous research has looked at the role of technical-related factors in improving ISA among users. Studies have a wide variety of interests in awareness-related variables that may not be within the vast area of education, training, and awareness. For example, the integrated model of Ramalingam et al. [46] used "Threat Awareness", "Password Awareness", and "Content Awareness"; Hanus and Wu [40] used "Threat Awareness" and "Countermeasure Awareness". Furthermore, Han [47] used "Security Technology Awareness"; Mamonov and Benbunan-Fich [48] used "Threat Awareness"; Khan and AlShare [49] used "information security policy scope". Moreover, Koohang et al. [50] used "Security Issues Awareness" and "Security Policy Awareness"; and Hwang et al. [51] used two separate constructs: "Security Policy" and "Security Education". According to Yaokumah et al. [52], security education benefits employees by improving their awareness of the organization's security environment, policies, and regulations. Effective training programmes may teach employees how to make secure information security choices. Staff security awareness programs may aid in the improvement of their security behaviour. Security education, training, and awareness (SETA) programs are educational and training programs designed to increase employees' knowledge of information security. These programs foster continued interest in rules and guidelines, risks, and the skills required to perform information systems security activities [21]. Consequently, rather than using the limited constructs of security awareness, the study prefers to use SETA as a construct with its complete and comprehensive concept of education, training, and awareness as compared to the limited constructs of security awareness. Employees may think they have the requisite knowledge and abilities to handle security issues in the workplace if they perceive SETA as effective. It stands to reason that employees with sufficient training are better equipped with skills and knowledge regarding security regulations and countermeasures. As a result, their behaviour will improve in order to comply with security policies. Hence, it is hypothesised that:

H8: SETA programs have a positive impact on the behavioural intentions of employees.

E. Behavioural Intention

One of the most significant constructs in TPB is the intention, which refers to the state of mind of a person in which the planning and forethought are to achieve a particular behaviour [3], [33]. According to the relevant studies, an individual's desire to achieve a goal that satisfies him or her yields an intention to participate in behaviour that encourages that goal. Bélanger et al. [14] and Thompson et al. [39] demonstrated that early conformity behavioural intention significantly predicts early conformity actual behaviour. In an attempt to predict the first adoption of information security behaviours, Ofori et al. [19] and Shropshire et al. [53] demonstrated a significant correlation between intention and actual behaviour. Although positive behavioural intentions toward a specific behaviour may ensure that the actual behaviour is achieved [51], intention alone may not adequately determine actual behaviour if explanatory power is not obtained by investigating both. Thus, it is hypothesised that:

H9: Employees' behavioural intentions towards ISA positively affect their adoption of InfoSec actual behaviour.

F. Facilitating Conditions Factors

External factors termed "facilitating conditions" (FC) are external factors outside the original theories. FCs are influential determinants that, along with other factors, promote a particular behaviour and are used to promote behavioural intention or actual behaviour to adopt technology [66]. These factors are included in the study's model to make an action easy to do. The study's model contains two constructs of facilitating conditions: organisational support [33] and InfoSec communication channels to promote employees' behaviour according to information security regulations. Organisational support indicates to employees; global beliefs about how an institution recognises and appreciates the employees' contributions and cares for their well-being. As Ofori et al. [19]; Khan and AlShare [49]; and Safa et al. [22] point out, organisations that show a commitment to their employees' well-being are better capable of protecting their assets through knowledge sharing and collaboration. Thus, it is hypothesised that:

H10: Organizational support towards employees facilitates their InfoSec's actual behaviour in accordance with information security policies.

Employee perception of the value of information and an organization's information security communication all contribute to the improvement of ISA through increasing knowledge of the importance of information security [1]. Moreover, employee communication channels regarding information security may reduce ambiguity and increase the frequency and usefulness of cross-functional communication, hence improving an individual's behaviour formation efficiency. Without formal communication channels, attitudes that violate safety norms would spread rapidly and prevent adopting correct ones [15]. According to Bélanger et al. [14], institutions may increase employee knowledge and awareness through targeted communications about the new need and justification for the recommended measures and security-related training. In terms of communication channels, this study asserts that effective communication amongst staff about all information security concerns and issues may help reduce human vulnerabilities associated with having adequate expertise to comply with applicable laws and regulations. Thus, good communication can help employees learn new skills, make better decisions, report incidents, and clear up misconceptions about information security [13]. Hence, it is hypothesised that:

H11: InfoSec communication channels positively affect employees' InfoSec actual behaviour.

III. Methodology

This study aims to demonstrate how public organisations can manage the human component and increase their ISA by examining factors such as prediction, control, motivation, deterrence, technical-related, and facilitating conditions for the adoption of InfoSec behaviour and reducing the risk of information security breaches. The success factors were designed to maximise employees' ISA by relying on constructs from TPB, PMT, and GDT, as well as three external factors. Hence, this study methodology adheres to a positivist philosophy, which involves identifying essential relationships relating to the phenomenon (in this instance, the adoption of InfoSec behaviour); it also adheres to a quantitative approach, which is implemented via the distribution of a questionnaire. Expert feedback was used to develop the research model. Quantitative approaches were also used to enhance the model. Because the research is aimed at public sector units' employees, data was gathered from public government organisations in the Sultanate of Oman. A questionnaire with a 5-point Likert scale was used to gather data.

A. Instrument Development and Data Collection

After consulting questions from relevant past research, the questions in the present study's questionnaire were constructed to correspond to the framework and constructs. The questionnaire was divided into two sections: the first included six questions on the participants' demographics, and the second included questions about the proposed model's variables, for a total of 71 questions. In the final form of the questionnaire, each component was addressed with different questions with various options ranging from strongly disagree to strongly agreed (Using a Likert scale of 5-points). Before distribution, a pilot study with 100 respondents was conducted to ensure the reliability of the questionnaire's items [16] and to determine whether the questionnaire's questions were appropriate, intelligible, and subject to a single interpretation. The current study's data collection started in the first week of January 2022 and was finished by the end of February 2022 (Over approximately seven weeks). After describing the purpose of the study to the participants, we asked them to answer the questionnaire based on their knowledge and experience. Their consent was necessary for the researchers. They were given the questionnaire after confirming their consent to participate in this research. Participants were informed that their responses would be used exclusively for statistical and scholarly reasons and would be kept private. The study used stratified random sampling, which divides a target population into smaller subgroups called "strata". Random samples are drawn from these groups based on how much of the target population they make up.

B. Participants' Demographic Characteristics

The Sultanate of Oman’s public sector employs 170,104 employees [54], making it one of the major sectors in the country. According to Krejcie and Morgan’s equation [55], a sample of at least 384 participants is necessary for this study’s intended population. Employees in the public sector were given 480 questionnaires, of which 415 were returned. The overall response rate was 86%, with 24 outliers. An overall response rate of 81% was obtained from the 391 validated responses. The remaining responses were discarded due to their repetitive answers or incompleteness. As shown in Table I, males comprised 248 (63.4%) of the total participants. The group over 40 years had the highest frequency of respondents’ age, with 119 (30.4%), followed by 31—35 years of age, with 112 (28.6%). A bachelor’s degree was the most often mentioned qualification among respondents (174; 44.5%). The most frequently occurring occupation among respondents (163; 34.8%) was “Employee”, followed by “Technician” (70; 17.9%). The group with more than ten years of experience had the highest frequency of responders with more than ten years of experience (208; 53.2%). Most respondents belonged to educational or service-related institutions, with 128 (32.7%) and 101 (25.78%), respectively.

TABLE I. Demographic Characteristics

Variables		**Frequency**	**%**
Gender	Male	248	63.4
	Female	143	36.6
Age (years)	25 or Less	20	5.1
	26 – 30	33	8.4
	31 – 35	112	28.6
	36 - 40	107	27.4
	Above 40	119	30.4
Education	Diploma	52	13.3
	High Diploma	82	21
	Bachelor	174	44.5
	Master	71	18.2
	Doctorate	12	3.1
Employment Situation	Employee	136	34.8
	Specialist	53	13.6
	Technician	70	17.9
	Chief-Employee	47	12
	Manager	30	7.7
	Other	55	14.1
Experiences	1 - 2	26	6.6
	3 - 5	48	12.3
	6 - 10	109	27.9
	Above 10	208	53.2
Organization	Education	128	32.7
	Health	75	19.2
	Service	101	25.8
	Other	87	22.3

IV. Results

A structured questionnaire adapted from prior studies was used to address the proposed conceptual model, which was then translated from English into Arabic and distributed to the target population. It was because the language of the survey had changed from one language to another that both exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) were used. SEM with AMOS version 24 was also used to see if the research hypotheses were accepted or rejected. Both measurement (MM) and structural (SM) models were developed in the study to model talent variables. They are two essential components used in the SEM to verify the study model's validity and reliability. The measurement model examines the relationship between latent constructs and their items to see if these indicators accurately measure the relevant talent construct. This step must be done before fitting the MM to the data to check the reliability and validity of the factor's items. In contrast, the structural model examines the relationships between one latent construct and other latent constructs [56].

A. Measurement Model Testing

SEM is a suitable approach for assessing data and estimating associations between constructs by accepting or rejecting formulated hypotheses to investigate the relationships between constructs in the study's model. SEM has many advantages, like isolating errors and estimating regression between latent constructs. Skewness and kurtosis tests were used to test the data distribution's normal state (normality); the study followed Hair et al. [57]'s recommendations and utilised a critical cut-off value of ±2.58. The results indicated that the skewness and kurtosis values for each model's variables were within the specified limits, indicating that the distribution is normal. For determining the suitability of factor analysis, Bartlett's test of sphericity (significant at $p<0.001$) and the Kaiser-Mayer-Olkin test (KMO) (values ranging between 0 and 1) were conducted. [58]. The KMO test score was 0.919, with a minimum suggested score of 0.50 and values greater than 0.9 were deemed excellent. The Chi-square statistic was significant (14100.952). The results of the KMO and Bartlett's tests are shown in Table II.

In line with relevant existing literature, the model for this study was constructed by incorporating the most successful parameters from three psychological theories and three external factors. Consequently, confirmatory factor analysis (CFA) is an important second step in evaluating whether the measured determinants align with our interpretation of the proposed model [59]. Furthermore, to develop the best potential measurement model, every item or latent variable that was not a good match (not fit) must be excluded [56]. The most frequent model-fit measures, according to Bollen [60], are the chi-square test (χ^2), comparative fix index (CFI), incremental fix index (IFI), Tucker-Lewis index (TLI), and root mean square error of approximation (RMSEA). Hence, in this study, these measures and the p-value were utilized as a goodness of fit indices to analyze the exogenous and endogenous variables. As a finding, χ^2 = (2558.954), degrees of freedom = (1346), ratio-χ^2/df = (1.901) less than 5, CFI = (.910), IFI = (.911), TLI = (.901), and RMSEA = (.048) less than 0.080, indicating that the measurement model was a good match (fit) with the data gathered [57]. Furthermore, the Root Mean Square Residual (RMR) = (0.037), less than 0.10. According to Table III, all model-fit indices surpassed the indicated acceptable thresholds.

The study used CFA to calculate the factor loading of the measurement variables to estimate the convergent viability. According to Hair et al. [57], if the loading factor of the indicators is more than 0.50 and the sample size is 300 or above, the loading factor shows an acceptable level of convergent validity. As a result, we removed indicators from the study's model with a factor loading of less than 0.50. Due to lower factor loadings (less than 0.50) or cross-loadings, the indicators SN1, SN5, and SN6 in subjective norms, PBC1 in perceived behavioural control, PV5 in perceived threat vulnerability, RE1, RE2 in response efficacy, PCOS1 in perceived sanctions certainty, PSOS1, PSOS2, and PSOS3 in perceived sanctions severity, SETA2 and SETA7 in security education, training, and awareness, BI7 in behavioural intention, OS1 in organisational support, and COM5 in InfoSec communication channels were eliminated from the proposed model. Internal consistency in the measuring of model variables is provided through reliability measurement. A questionnaire's reliability (Cronbach's alpha) is thought to be accepted when it is more than 0.6 [61], and when it is above 0.7, it is indicated to be composite reliability [56]. The two kinds of reliability testing were used in this analysis. Cronbach's alpha scores vary from 0.807 to 0.908, while composite reliability scores range from 0.814 to 0.901. As a result, the reliability and composite reliability values for the entire model's variables were more than 0.7. Table IV provides an overview of the statistical measurements.

TABLE II. The KMO and Bartlett's Test Results

Measurement of Sampling Adequacy: Kaiser-Meyer-Olkin	0.919	
Bartlett's Sphericity Test	**Approx. Chi –Square**	14100.952
	Df	1485
	Sig	.000

TABLE III. MM and SM Fit Indices

Fit Index	**Cut-off Points**	**MM**	**SM**
X^2	-	2558.954	3378.335
d.f	-	1346	1393
Ratio (X^2/d.f)	<5	1.901	2.425
CFI	>0.90	.910	.853
IFI	>0.90	.911	.854
TLI	>0.90	.901	.850
RMSEA	<0.08	.048	.060
RMR	<0.10	0.037	-

TABLE IV. THE VARIABLES, MEASURES, AND THEIR DESCRIPTIVE STATISTICS

Variables	**Items**	**Measures**	**Factor Loading**	**AVE**	**Alpha**	**CR**
InfoSec Attitude	ATT1	Information security awareness is necessary.	0.773	0.514	0.870	0.862
	ATT2	Information security awareness is beneficial.	0.877			
	ATT3	Practicing information security awareness activities is useful.	0.754			
	ATT4	I believe that information security awareness is a useful behavioural tool to safeguard the organization's information assets.	0.633			
	ATT5	My information security awareness has a positive effect on mitigating the risk of information security breaches.	0.624			
	ATT6	Information security awareness is a wise approach that decreases the risk of information security incidents.	0.624			
Subjective Norms	SN2	My colleagues think that I should have information security awareness to protect organizational information assets.	0.685	0.545	0.864	0.781
	SN3	My friends in my office encourage me to understand information security policies.	0.699			
	SN4	The head of the department thinks that information security awareness is a value culture	0.822			
Perceived Behavioural Control	PBC2	I have the necessary awareness about information security to share with the other employees.	0.766	0.636	0.873	0.875
	PBC3	I have the ability to adopt information security awareness to mitigate the risk of information security breaches.	0.804			
	PBC4	Information security awareness adoption is an easy and enjoyable task for me.	0.803			
	PBC5	I have enough knowledge to behave safely in terms of information security.	0.817			
Response Efficacy	RE3	At my work, efforts to ensure the safety of my confidential information are effective.	0.668	0.661	0.858	0.852
	RE4	The preventative measures available to me to stop people from gaining access to my organization's information are adequate.	0.880			
	RE5	The preventative measures available to me to prevent people from damaging my information system at work are adequate.	0.873			
Perceived Threat Vulnerability	PV1	I know my organization could be vulnerable to security breaches if I don't adhere to its information security policy.	0.755	0.524	0.812	0.814
	PV2	I could fall victim to a malicious attack if I fail to comply with my organization's information security policy.	0.727			
	PV3	I believe that trying to protect my organization's information will reduce illegal access to it.	0.673			
	PV4	My organization's data and resources may be compromised if I don't pay adequate attention to guidelines.	0.737			
Behavioural Intention	BI1	I am willing to practice my information security awareness because of its potential to reduce the risks.	0.674	0.501	0.872	0.857
	BI2	I will share my information security awareness with my colleagues to comply with security policies.	0.734			
	BI3	I intend to help my colleagues to increase their awareness of information security	0.776			
	BI4	I intend to collaborate with other staff to decrease insider threats in my organization.	0.699			
	BI5	I will inform the other staff about new methods and software that can reduce the risk of information security.	0.686			
	BI6	I will share the report on information security incidents with others, in order to reduce the risk.	0.665			
InfoSec Actual Behaviour	AB1	I frequently practice my experience about information security with my colleagues.	0.663	0.505	0.908	0.901
	AB2	I practice my information security knowledge with my colleagues.	0.653			
	AB3	I frequently share my expertise from my information security training with my colleagues.	0.680			
	AB4	I frequently talk with others about information security incidents and their solutions in our meetings.	0.709			
	AB5	I avoid mistakes in the domain of information security.	0.783			

	AB6	I always mitigate information security threats.	0.785			
	AB7	I think about the consequences of my behaviour before any action.	0.666			
	AB8	I am careful about my behaviour in the domain of information security.	0.642			
	AB9	I frequently assess my information security behaviour to improve it.	0.750			
Perceived Certainty of Sanctions	PCOS2	I believe that if I violate the confidentiality of information, the management will realise it.	0.769	0.640	0.866	0.875
	PCOS3	If I violated the organization's security policies, I would probably be caught.	0.624			
	PCOS4	I believe that if I transfer organisational information outside, the organisation will find out about my violation.	0.907			
	PCOS5	I believe that if I sell organisational information, my organisation will discover it.	0.870			
Perceived Severity of Sanctions	PSOS4	I deserve punishment if I violate the confidentiality of organisational information.	0.782	0.605	0.807	0.820
	PSOS5	I think punishment will be high if I sell or transfer organisational information outside.	0.854			
	PSOS6	I think receiving sanctions because of my information security misconduct will negatively influence my career development.	0.688			
Organizational Support	OS2	The organisation cares about my information security awareness level.	0.839	0.654	0.863	0.883
	OS3	The management appreciates employees for their information security awareness.	0.805			
	OS4	The management awards employees for their compliance with information security policies.	0.766			
	OS5	The management encourages employees to participate in information security awareness engagement.	0.824			
InfoSec Communication Channels	COM1	We have communication channels established for employees to report information security suspected improprieties.	0.755	0.669	0.875	0.889
	COM2	The management communicates employees' security duties and control responsibilities in an effective manner.	0.922			
	COM3	Communication flows across the organisation adequately (e.g., from department to department) to enable employees to discharge their responsibilities securely and efficiently.	0.753			
	COM4	I feel as though I am a part of the information security decision-making process within my organization.	0.727			
Security Education, Training and Awareness	SETA1	My organization gives employees training to help them become more aware of information system security issues.	0.610	0.568	0.866	0.866
	SETA3	SETA increases my knowledge of security issues.	0.752			
	SETA4	SETA motivates the learners to integrate the security knowledge taught.	0.855			
	SETA5	My organisation provides employees with appropriate security education before giving them authorised access to the institution's network.	0.844			
	SETA6	My organization utilizes various communication methods in order to improve the information security awareness of employees.	0.679			

TABLE V. CORRELATION ANALYSIS AND DISCRIMINANT VALIDITY

	AVE	MSV	PV	PBC	OS	PCOS	COM	SETA	ATT	SN	AB	PSOS	RE	BI
PV	0.524	0.309	**0.724**											
PBC	0.636	0.530	0.390	**0.798**										
OS	0.654	0.605	0.343	0.509	**0.809**									
PCOS	0.640	0.411	0.416	0.430	0.641	**0.800**								
COM	0.669	0.605	0.368	0.490	0.778	0.617	**0.818**							
SETA	0.568	0.378	0.372	0.615	0.610	0.485	0.562	**0.754**						
ATT	0.514	0.131	0.362	0.174	-0.077	0.017	0.023	0.167	**0.717**					
SN	0.545	0.041	-0.026	-0.203	-0.194	-0.201	-0.197	-0.174	0.058	**0.738**				
AB	0.505	0.500	0.505	0.728	0.643	0.475	0.575	0.588	0.117	-0.146	**0.710**			
PSOS	0.605	0.279	0.528	0.289	0.383	0.494	0.385	0.374	0.268	-0.066	0.523	**0.778**		
RE	0.661	0.444	0.385	0.652	0.657	0.515	0.618	0.586	0.005	-0.078	0.666	0.290	**0.813**	
BI	0.501	0.462	0.556	0.475	0.528	0.344	0.379	0.460	0.330	0.044	0.680	0.485	0.442	**0.707**

Note: PV = Perceived Threat Vulnerability, PBC = Perceived Behavioural Control, OS = Organizational Support, PCOS = Perceived Certainty of Sanctions, COM = InfoSec Communication Channels, SETA = Security Education, Training and Awareness, ATT = InfoSec Attitude, SN = Subjective Norms, AB = InfoSec Actual Behaviour, PSOS = Perceived Severity of Sanctions, RE = Response Efficacy, BI = Behavioural Intention.

Discriminant validity is realized when a construct is remarkably different from the other constructs since there is no association between constructs that do not relate to each other [57]. The square root of the AVE was more significant than the correlations between the construct and the other model's constructs, which varied between 0.017 and 0.778 for the given model. Moreover, the maximum shared squared variance (MSV) was smaller than the AVE. Thus, the discriminant validity verification supported all of the model's constructs. Table V displays the matrices of correlation between various latent variables.

B. Structural Model Testing

In this study, the same set of fit indices is used to analyse the structural model. As indicated in Table III, all fit indices were within the acceptable ranges: χ^2 = (3378.335), degrees of freedom= (1393), ratio-χ^2/df= (2.425), RMSEA = (.060), with the exception of CFI = (.853), IFI = (.854), and TLI = (.850). However, another method of evaluating the values derived from the CFI, IFI, and TLI indices should be considered. According to Bentler and Bonett [62] and Sharma et al. [63], the TLI cut-off point is continually shifting. Since there is no globally approved measuring standard, a TLI value between 0.80 and 0.90 may be considered a moderate or acceptable fit. Bentler [64] believed that CFI indicates a good fit when it equals or surpasses 0.90, while values larger than 0.80 and reaching 0.90 suggest a generally adequate fit, and Bollen [60] made the same suggestion for IFI index values. Moreover, Schumacher and Lomax [65] state that if the IFI, CFI, and ITL values are greater than 0.90, they are considered excellent fits, but they may also be considered moderate if the values are between 0.85 and 0.90. As a result of the above, we believe that the model is both appropriate and a good match for the data, as the parsimonious index provides the most accurate measurement (RMSEA= .060).

TABLE VI. STRUCTURAL MODEL CAUSAL PATHS

Paths	**Standardized estimate (*β*)**	**P-value**	**Result**
ATT → BI	0.138	0.009	Supported
SN → BI	0.146	0.020	Supported
PBC → BI	0.300	0.000	Supported
PV → BI	0.311	0.000	Supported
RE → BI	0.148	0.045	Supported
PCOS → BI	-0.107	0.106	Rejected
PSOS → BI	0.276	0.000	Supported
SETA → BI	0.139	0.000	Supported
BI → AB	0.582	0.000	Supported
OS → AB	0.262	0.001	Supported
COM → AB	0.187	0.015	Supported

Note: ATT = InfoSec Attitude, SN = Subjective Norms, PBC = Perceived Behavioural Control, RE = Response Efficacy, PV = Perceived Threat Vulnerability, PCOS = Perceived Certainty of Sanctions, PSOS = Perceived Severity of Sanctions, SETA = Security Education, Training and Awareness, BI = Behavioural Intention, OS = Organizational Support, COM = InfoSec Communication Channels, AB = InfoSec Actual Behaviour.

The findings of the causal paths are shown in Table VI. Employees' ISA behavioural intention was significantly influenced by InfoSec attitude (*β*=0.137, p=0.009), subjective norms (*β*=0.107, p=0.048), perceived behavioural control (*β*=0.296, p=0.000), response efficacy (*β*=0.148, p=0.018), perceived threat vulnerability (*β*=0.297, p=0.000), perceived sanctions severity (*β*=0.274, p=0.000), and security education, training, and awareness (*β*=0.139, p=0.000). On the other hand, the impact of perceived sanctions certainty on employees' ISA behavioural intentions was insignificant. As a result, H6 is rejected. Finally, the results demonstrated that ISA behavioural intention (*β*=0.584, p=0.000), InfoSec communication channels (*β*=0.188, p=0.015), and organizational support (*β*=0.262, p=0.001) all had a significant impact on InfoSec actual behaviour adoption.

V. Comparative Evaluation of the Study Model

The study's significance derives from the inclusion of control, prediction, motivation, and deterrence approaches, all resulting from three main theories: TPB, PMT, and GDT. This study investigated whether the TPB affected intentions in information security behaviour adoption among public organisation employees and revealed that the TPB has a good to excellent effect, supporting results of previous studies [3], [18], [27], [28] and contradicting the findings of Rajab and Eydgahi's [2] study. The presented factors encourage institutions' employees to engage in ISA activities and, consequently, InfoSec behaviour adoption. The results of the InfoSec attitude analysis indicated that employees who expect advantages from ISA activities are more likely to adopt InfoSec behaviours consistent with their understanding of ISA. As a consequence of our analysis of subjective norms, we can assume that employees get cooperation about their engagement in ISA activities from their managers, supervisors, and co-workers. The present case demonstrates the significance of perceived behavioural control, which indicates that controlling perceptions may impact employees' intentions, allowing ISA activities to effectively engage in a suitable work environment. Because PMT is a practical framework for estimating an employee's intention to take preventive measures, some studies indicate that perceived vulnerability [17], [39] and response efficacy [40], [41] related to information security have a significant impact on information security policy compliance. This study found that almost all of their findings align with these findings. The study also found PMT to be among the best theoretical frameworks for explaining ISA intentions toward InfoSec behaviour adoption, which is consistent with previous results [17], [36], [39]. The purpose of GDT constructs is to treat employee criminal behaviour. The target of applying sanctions is to prevent or eliminate undesirable employee conduct. The imposition of sanctions helps to alter the behaviour of uncooperative staff to some degree [44] and raises awareness of illegal behaviour among other employees when penalties are implemented. As proven by prior studies [19], [27], [43], there is a significant positive relationship between the severity of sanctions and compliance with information security policies. While the results of this study confirm the findings of earlier research on the sanctions' severity and InfoSec's behaviour through ISA intention, they also suggest that as the likelihood of sanction severity rises, employees' intentions for InfoSec behaviour rise as well. Jaeger et al. [27] discovered that the sanctions' certainty did not affect the variance in information security policy compliance, which confirms the results of this study. The study targeted public sector employees as a possible explanation for this non-significant relationship. This sector most certainly differs from the private sector in several ways; for example, employees in this sector work in a more stable environment, which may lower their motivation compared to private sector employees. Employees in the public sector might need more powerful ways to get them excited, such as recognition and responsibility.

The study's findings reveal that SETA programs strongly affect public institution employees' ISA intentions towards InfoSec behaviour. According to prior studies, SETA programs motivate employees to follow information security policies and procedures [20], [21]. When public sector employees get appropriate SETA programs, they will gain an essential awareness of security knowledge and abilities. They will also be able to show their commitment to the information security policy through their behaviour. Accordingly, they will be one of the most effective defence lines in safeguarding information assets and professionally responding to risks and attacks. Furthermore, the results showed that a positive ISA intention toward adopting InfoSec behaviour, organisational support, and InfoSec communication channels affected employees' adoption of InfoSec behaviour. The statistical analysis and the literature review show that the proposed model is both sound and efficient. A model for adopting information security behaviours in public organisations was contributed by determining the success factors that would influence the intentions of public sector employees to engage in ISA activities and adopt best behavioural practices. It is expected that the results of this research will be used by content development consultants to improve and enhance ISA materials and by SETA program developers and designers to prepare and design ISA and best practices programs and initiatives. The proposed model concentrates on the two aspects of behavioural intentions and actual behaviour to add to existing knowledge on ISA and best practices. In addition, it includes the facilitating conditions that positively influence employees' ISA (i.e., Organisational support and InfoSec communication channels) to enhance and correct actual behaviour in the process of ISA.

This study is one of the studies that envision increasing employee awareness and understanding of information security and reducing breaches through a combination of factors. This aggregation creates a new perspective that helps public institutions more effectively manage human ISA. We believe this research adds to this field's existing body of knowledge.

VI. Conclusion, Limitations and Future Work

The fast growth of information technology has made it simpler, more accurate, and more efficient to carry out organisational functions. Nevertheless, there is still a gap between how far technology has advanced and how much employees are aware of it, making it challenging for public institutions to preserve their assets. A lack of users' ISA causes many security risks and challenges. Through this study, we seek to strengthen and broaden research on the challenges of ISA in organisations by leveraging success factors extracted from three theories established on the principles of control, prediction, motivation, and deterrence. Public institutions may influence their employees' intentions to align with desired information security behaviour by employing control and prediction factors. Employees are also encouraged by motivational factors to practice security countermeasures and continuously maintain their knowledge and skills. Deterrence factors contribute to the control of criminal wrongdoing and, through them, can spread security awareness via understanding criminal behaviour. Usually, there are two aspects to SETA programs: the fundamental part and the institutional-specific. The fundamental part of all SETA programs is to determine and monitor the critical human threats and risks and employee behaviours linked to those threats and risks. The institutional-specific part is designed to address the requirements of employees and the institution. The institution's recognised risks and behaviours should influence the awareness efforts. Employees must be provided with these programs consistently. They must also be consistently evaluated. Furthermore, the research model has been expanded to include facilitating conditions that help make sure that actual InfoSec behaviour is in line with information security regulations and policies.

To further extend this study, it is necessary to identify the determinants that influence employees' engagement in ISA activities, their difficulties and obstacles, and their perspectives on them. Future studies might look at the implementation of ISA through alternative models and theories and extend the technical, organisational, environmental, and individual factors. Additionally, interviews and group discussions might be conducted to ascertain any underlying reasons for the lack of ISA, particularly in public institutions. Among the study's limitations is that it focused only on public-sector units in Oman. Consequently, the findings do not accurately reflect the behaviour of other sectors, such as the private, industrial, and financial sectors, resulting in a lack of representation. Future studies can incorporate a diverse range of sectors into their study sample.

Acknowledgment

This publication has been funded under the industrial grant INDUSTRI/APSB/FTMK/2021/I00063. The authors would like to thank UTeM and Ask Pentest Sdn Bhd research group members for their support.

References

[1] K. Khando, S. Gao, S. Islam and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review", *Computers & Security*, vol. 106, p. 102267, 2021.

[2] M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education", *Computers &amp; Security*, vol. 80, pp. 211-223, 2019.

[3] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh, and M. Sookhak, "Deterrence and prevention-based model to mitigate information security insider threats in organisations", *Future Generation Computer Systems*, vol. 97, pp. 587-597, 2019.

[4] C. Cybersecurity, "ENISA threat landscape report 2018 : 15 top cyber-threats and trends.", *Op.europa.eu*, 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/6373c334-574d-11e9-a8ed-01aa75ed71a1/language-en. [Accessed: 03- May- 2022].

[5] N. Humaidi and V. Balakrishnan, "Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information

Security Awareness", *International Journal of Information and Education Technology*, vol. 5, no. 4, pp. 311-318, 2015.

[6] T. Sommestad, "Work-related groups and information security policy compliance", *Information & Computer Security*, vol. 26, no. 5, pp. 533-550, 2018. Available: 10.1108/ics-08-2017-0054.

[7] L. Li, W. He, L. Xu, I. Ash, M. Anwar and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, vol. 45, pp. 13-24, 2019.

[8] F. Haeussinger and J. Kranz, "Antecedents of employees' information security awareness - review, synthesis, and directions for future research", *AIS Electronic Library (AISeL)*, 2022. [Online]. Available: https://aisel.aisnet.org/ecis2017_rp/12/. [Accessed: 03- May- 2022].

[9] M. Siponen, M. Adam Mahmood and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study", *Information & Management*, vol. 51, no. 2, pp. 217-224, 2014.

[10] R. Vaidya, "Cyber Security Breaches Survey 2019", *Department for Digital, Culture, Media and Sport*, 2019. [Online]. Available: https://drj.com/wp-content/uploads/2019/04/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF. [Accessed: 03- Apr- 2022].

[11] L. Jaeger, "Information security awareness: literature review and integrative framework", in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[12] J. Abawajy, "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237-248, 2014.

[13] M. Bada, A. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" in *International Conference on Cyber Security for Sustainable Society*, 2019.

[14] F. Bélanger, S. Collignon, K. Enget and E. Negangard, "Determinants of early conformance with information security policies", *Information & Management*, vol. 54, no. 7, pp. 887-901, 2017.

[15] Y. Hong and S. Furnell, "Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization", *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 19-28, 2022.

[16] I. Al-Shanfari, W. Yassin, R. Abdullah, N. Al-Fahim and R. Ismail, "Introducing A Novel Integrated Model for the Adoption of Information Security Awareness through Control, Prediction, Motivation, and Deterrence Factors: A Pilot Study", *Journal of Theoretical and Applied Information Technology*, vol. 99, no. 1, pp. 2991–3003, 2021.

[17] C. Howell, "Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization", Doctoral dissertation, University of South Florida, 2021.

[18] T. Grassegger and D. Nedbal, "The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering", *Procedia Computer Science*, vol. 181, pp. 59-66, 2021. Available: 10.1016/j.procs.2021.01.103.

[19] K. Ofori, H. Anyigba, G. Ampong, O. Omoregie, M. Nyamadi and E. Fianu, "Factors influencing information security policy compliance behavior", in *Research Anthology on Business Aspects of Cybersecurity*, 2022, pp. 213-232.

[20] K. Kuo, P. Talley and D. Lin, "Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables", *INQUIRY: The Journal of Health Care Organization, Provision, and Financing*, vol. 58, pp. 1-12, 2021.

[21] H. Kim, H. Choi and J. Han, "Leader power and employees' information security policy compliance", *Security Journal*, vol. 32, no. 4, pp. 391-409, 2019.

[22] N. Sohrabi Safa, C. Maple, T. Watson and S. Furnell, "Information security collaboration formation in organisations", *IET Information Security*, vol. 12, no. 3, pp. 238-245, 2018.

[23] P. Kuppusamy, G.N. Samy, N. Maarop, P. Magalingam, N. Kamaruddin, B. Shanmugam, and S. Perumal, "Systematic Literature Review of Information Security Compliance Behaviour Theories", *Journal of Physics: Conference Series*, vol. 1551, no. 1, p. 012005, 2020.

[24] M. Alassaf and A. Alkhalifah, "Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review", *IEEE Access*, vol. 9, pp. 162687-162705, 2021.

[25] T. Gundu and S. Flowerday, "Ignorance to Awareness: Towards an Information Security Awareness Process", *SAIEE Africa Research Journal*, vol. 104, no. 2, pp. 69-79, 2013.

[26] A. Burns, T. Roberts, C. Posey, R. Bennett and J. Courtney, "Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts", *Decision Sciences*, vol. 49, no. 6, pp. 1187-1228, 2017.

[27] L. Jaeger, A. Eckhardt and J. Kroenung, "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis", *Information & Management*, vol. 58, no. 3, p. 103318, 2021.

[28] Y. Hong and S. Furnell, "Organizational formalization and employee information security behavioral intentions based on an extended TPB model", in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2019, pp. 1-4.

[29] L. Ong and C. Chong, "Information Security Awareness: An Application of Psychological Factors–A Study in Malaysia", in *2014 International Conference on Computer, Communications and Information Technology (CCIT 2014)*, 2014, pp. 98-101.

[30] B. Khan, K. Alghathbar, S. Nabi and M. Khan, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, vol. 5, no. 26, pp. 10862-10868, 2011.

[31] A. Ahlan, M. Lubis and A. Lubis, "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures", *Procedia Computer Science*, vol. 72, pp. 361-373, 2015.

[32] N. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. Ghani and T. Herawan, "Information security conscious care behaviour formation in organizations", *Computers & Security*, vol. 53, pp. 65-78, 2015. http:10.1016/j.cose.2015.05.012.

[33] N. Safa and R. Von Solms, "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, vol. 57, pp. 442-451, 2016. Available: 10.1016/j.chb.2015.12.037.

[34] I. Ajzen, "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179-211, 1991.

[35] A. Onumo, I. Ullah-Awan and A. Cullen, "Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures", *ACM Transactions on Management Information Systems*, vol. 12, no. 2, pp. 1-29, 2021. Available: 10.1145/3424282.

[36] L. Li, L. Xu and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior", *Computers in Human Behavior Reports*, vol. 5, p. 100165, 2021. Available: 10.1016/j.chbr.2021.100165.

[37] R. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1", *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, 1975. Available: 10.1080/00223980.1975.9915803.

[38] S. Boss, D. Galletta, P. Lowry, G. Moody and P. Polak, "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors", *MIS Quarterly*, vol. 39, no. 4, pp. 837-864, 2015. Available: 10.25300/misq/2015/39.4.5.

[39] N. Thompson, T. McGill and X. Wang, "“Security begins at home”: Determinants of home computer and mobile device security behavior", *Computers &amp; Security*, vol. 70, pp. 376-391, 2017. Available: 10.1016/j.cose.2017.07.003.

[40] B. Hanus and Y. Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective", *Information Systems Management*, vol. 33, no. 1, pp. 2-16, 2015. Available: 10.1080/10580530.2015.1117842.

[41] M. Martens, R. De Wolf and L. De Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general", *Computers in Human Behavior*, vol. 92, pp. 139-150, 2019. Available: 10.1016/j.chb.2018.11.002.

[42] M. Stafford, "Deterrence Theory: Crime", *International Encyclopedia of the Social & Behavioral Sciences*, pp. 255-259, 2015. Available: 10.1016/b978-0-08-097086-8.45005-1 [Accessed 4 May 2022].

[43] N. Ameen, A. Tarhini, M. Hussain Shah and N. Madichie, "Employees' behavioural intention to smartphone security: A gender-based, cross-national study", *Computers in Human Behavior*, vol. 104, p. 106184, 2020. Available: 10.1016/j.chb.2019.106184.

[44] B. Lebek, J. Uffen, M. Neumann, B. Hohler and M. Breitner, "Information security awareness and behavior: a theory-based literature review", *Management Research Review*, vol. 37, no. 12, pp. 1049-1092, 2014. Available: 10.1108/mrr-04-2013-0085.

[45] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?", *Information Systems Management*, vol. 33, no. 1, pp. 30-41, 2015. Available: 10.1080/10580530.2015.1117868.

[46] R. Ramalingam, R. Lakshminarayanan and S. Khan, "Information Security Awareness at Oman Educational Institutions : An Academic Prespective", *arXiv.org*, 2016. [Online]. Available: https://arxiv.org/abs/1605.05580. [Accessed: 13- Mar- 2022].

[47] B. Han, "User's Information Security Awareness in BYOD Programs: A Theoretical Model", in *Information Institute Conference*, 2017.

[48] S. Mamonov and R. Benbunan-Fich, "The impact of information security threat awareness on privacy-protective behaviors", *Computers in Human Behavior*, vol. 83, pp. 32-44, 2018. Available: 10.1016/j.chb.2018.01.028.

[49] H. Khan and K. AlShare, "Violators versus non-violators of information security measures in organizations—A study of distinguishing factors", *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 1, pp. 4-23, 2019. Available: 10.1080/10919392.2019.1552743.

[50] A. Koohang, J. Anderson, J. Nord and J. Paliszkiewicz, "Building an awareness-centered information security policy compliance model", *Industrial Management & Data Systems*, vol. 120, no. 1, pp. 231-247, 2019. Available: 10.1108/imds-07-2019-0412.

[51] I. Hwang, R. Wakefield, S. Kim and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior", *Journal of Computer Information Systems*, vol. 61, no. 4, pp. 345-356, 2021. Available: 10.1080/08874417.2019.1650676.

[52] W. Yaokumah, D. Walker and P. Kumah, "SETA and Security Behavior", *Journal of Global Information Management*, vol. 27, no. 2, pp. 102-121, 2019. Available: 10.4018/jgim.2019040106.

[53] J. Shropshire, M. Warkentin and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security*, vol. 49, pp. 177-191, 2015. Available: 10.1016/j.cose.2015.01.002.

[54] MOL, "Annual Report in the Civil Service Sector", *Staff.mol.gov.om*, 2021. [Online]. Available: https://staff.mol.gov.om/DSMVD/CMS/WebSiteMediaAnnual/07102021%20075839%20%D8%B5_vgyrm04r440la3h1sy3ksqin20219202175835(stat%202020).pdf. [Accessed: 14-Jan- 2022].

[55] R. Krejcie and D. Morgan, "Determining Sample Size for Research Activities", *Educational and Psychological Measurement*, vol. 30, no. 3, pp. 607-610, 1970. Available: 10.1177/001316447003000308.

[56] J. Hair, *Multivariate data analysis*. Englewood Cliffs, NJ: Prentice Hall, 2010.

[57] J. Hair, C. Ringle and M. Sarstedt, "Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance", *Long Range Planning*, vol. 46, no. 1-2, pp. 1-12, 2013. Available: 10.1016/j.lrp.2013.01.001.

[58] H. Kaiser, "An index of factorial simplicity", *Psychometrika*, vol. 39, no. 1, pp. 31-36, 1974. Available: 10.1007/bf02291575.

[59] R. Ho, *Handbook of univariate and multivariate data analysis and interpretation with SPSS*, 1st ed. Boca Raton, Fla: Chapman & Hall/CRC, 2006.

[60] K. Bollen, "A New Incremental Fit Index for General Structural Equation Models", *Sociological Methods & Research*, vol. 17, no. 3, pp. 303-316, 1989. Available: 10.1177/0049124189017003004.

[61] U. Sekaran, "Towards a guide for novice research on research methodology: Review and proposed methods", *Journal of Cases of Information Technology*, vol. 8, no. 4, pp. 24-35, 2003.

[62] P. Bentler and D. Bonett, "Significance tests and goodness of fit in the analysis of covariance structures.", *Psychological Bulletin*, vol. 88, no. 3, pp. 588-606, 1980. Available: 10.1037/0033-2909.88.3.588.

[63] S. Sharma, S. Mukherjee, A. Kumar and W. Dillon, "A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models", *Journal of Business Research*, vol. 58, no. 7, pp. 935-943, 2005. Available: 10.1016/j.jbusres.2003.10.007.

[64] P. Bentler, "Comparative fit indexes in structural models.", *Psychological Bulletin*, vol. 107, no. 2, pp. 238-246, 1990. Available: 10.1037/0033-2909.107.2.238.

[65] R. Schumacker and R. Lomax, *A beginner's guide to structural equation modeling*. psychology press, 2004.

[66] H. Triandis, "Values, attitudes, and interpersonal behavior", in *Nebraska Symposium on Motivation*, 1979, pp. 195-259.

[67] I. Al-Shanfari, W. Yassin, R. Abdullah, "Identify of Factors Affecting Information Security Awareness and Weight Analysis Process", *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 3, pp. 534-42, 2020.