International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Identify of Factors Affecting Information Security Awareness and Weight Analysis Process

Issam Al-Shanfari, Warusia Yassin, Raihana Abdullah

Abstract: ***Information exchange is a key aspect of using technology in everyday life. Crimes associated with the lack of information security awareness (ISA), misuse and carelessness are on the increase and often result in heavy losses and serious consequences. In order for ISA campaigns and programmes to be effective, the most successful and influential factors must be employed in the human component of the security awareness process. The purpose of this study is to investigate the causes of human breaches to information security and undertake a weight analysis of the models' predictors' relationships utilised in ISA literature from the current decade. Usable data were collected from twenty-one empirical studies related to ISA research in order to obtain the correlations required to perform a weight analysis process for a predictor's relationships. The relationships examined in all studies used in this research (significant–non-significant) are presented in a diagram. Findings show that six independent variables were found to be classified as 'well-utilised' variables, and the rest of the independent variables converge at the 'Promising' classification level. Contributions, limitations and directions of future work are presented.***

Keywords: Information Security awareness, ISA Success Factors, ISA Predictors, ISA Constructs, Weight Analysis.

I. INTRODUCTION

The rise in cybercrime around the world is an alarming problem. Statistics on the 2019 Internet World Stats point to an increase in the number of Internet users in the Middle East [1], where the percentage of users in Oman is (2.3%) of the total number of Internet users in the Middle East, which exceeds (3.9%) of the global number of Internet users. In recent years, Oman has emerged as one of the most important e-commerce markets in the Middle East due to the existence of excellent consumer protection laws enacted by the Omani authorities. The widespread use of Internet, smart phones and an increased number of online retailers has boosted economic growth in Oman due to its improved infrastructure and increased use of the Internet, especially by young people [2]. Continuous economic growth also led to an increase in the volume of Internet and mobile banking. These improvements in the payment infrastructure led to an increase in the volume of electronic transactions through banking debit cards to 1,932,224 electronic transactions, with a total revenue of RO 365 million at the end of 2017 [3].

The growing demand in Internet services also led to an increased use of debit cards in order to complete financial electronic transactions, including thirty-four Omani government entities that utilised e-payment services in 2017 [3]. Approximately ninety-three entities have launched electronic payment portal with their services , and nine government entities and government-owned companies joined the electronic payment gateway in order to use the Tenders Board's e-Tendering portal, where the number of charities and specialised organisations beneficiaries of electronic payment gateway services to twenty-seven institutions [3].

As we are in an era of technological advancement, new and innovative threats are constantly evolving, such as identity theft, phishing, spam, data leakage, intrusion, and many other dangers to individuals' privacy and organisational assets [4]. Attackers rely on more stealthy and advanced techniques to exploit victims' trust; they often use strategies that lead to weakness that the victim cannot predict, thus breaking privacy and getting access to confidential information. The gap between knowledge and the best security practices to be followed is often the main factor which affects both organisational assets and security of information.

Employee records, payroll data, patient medical records, and student grade records that contain a vast amount of sensitive and secret data are valuable assets to any organisation just like intellectual property, software, applications, websites, systems, network devices and computers. In general, these valuable assets are subject to a greater risk for data breaches and any other potential risks of information technology [4].

According to Bulgurcu et al [5], users' attitudes and beliefs are affected according to their level of information security awareness (ISA), which in turn positively or negatively affects their compliance with information security policies. Merete et al [6] stated that information security measures could not be effective unless staff members were sufficiently adept in ISA. Many statistics also indicate that victims of cybercrime are often users with insufficient ISA, even end users, so the number of victims of these crimes increases daily [7].

Creating security awareness and adopting best practices for information security among users is one of the best approaches to prevent or limit security breaches and cybercrime.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Issam Al-Shanfari*, PhD student, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) Durian Tunggal, Melaka, email: issam.moshaded@gmail.com

Dr. Warusia Yassin, Senior lecturer, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, email: s.m.warusia@utem.edu.my

Dr. Raihana Abdullah, Senior lecturer, Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Durian Tunggal, Melaka, email: raihana.syahirah@utem.edu.my

Therefore, in order to create cyber security awareness in the Sultanate of Oman, it is necessary to know the psychological factors influencing the creation of sufficient and effective user awareness. These factors must take into account the changing needs of people; they must consider people's patterns and daily cultural practices. Considering these factors, this paper has reviewed various studies that show reasons for the most common information security breaches among end users; the paper has also reviewed models and frameworks utilised in ISA literature showing the psychological factors affecting the creation of ISA among users, followed by a diagram of the relationships between variables and their weight analysis table.

II. BACKGROUND

Different cyber-attacks, especially social engineering attacks are flexible and can be changed in different ways. Security experts describe these kinds of attacks as a transmittable disease which has ability to adapt into new styles each time it is detected [8]. From this perspective, it is clear that how this kind of attack poses a major threat and is difficult to defend against, even to those users with fundamental ISA. Examples of this can be seen in recent times, such as attack on Bank Muscat customers in 2013 [9], and attack on several Omani public sector entities and individuals in 2016, where losses amounted to 90 million dollars, in addition to attacks on large groups of customers of various local banks in Oman by use of devices to capture clients' credit and debit card information, leading to embezzlements totalling up to OMR 525,000 [10].

The Information Technology Authority (ITA) annual report [3] indicated that there has been an increase in the number of cybercrime incidents and attempts, where an Oman National Computer Emergency Readiness Team (OCERT) has handled 880,843,349 cybercrimes against government networks and 1,411,043 cyber-attacks against government websites. A total of 44,340 cyber security attacks detected were targeting Omani cyberspace, and a total of 2,459 real cyber security incidents reported by government entities and citizens were handled. The OCERT also handled 626 malware infections resulting from the analysis of millions of attempted attacks against Omani cyberspace, and 172 digital forensics cases, which were handled using 877 evidence devices, resulted from cybercrimes in Oman [3]. One of the main reasons for the threat to information security in the organisation is a lack of ISA, employees' negligence and carelessness, or lack of education, training and awareness programmes. Even if such programmes existed, they often lack employment of the most psychological factors that influence the level of ISA among employees [7]. Although most Omani administrative and technical personnel have basic knowledge of information security, they are frequently unaligned with the security policies imposed by their organisations – there seems to be a lack of perception and understanding about the protection of secret information and organisational assets [4]. Therefore, it is important to determine and identify psychological factors of the human component that influence raising the ISA in Oman after investigating causes of employee-generated security breaches.

III. METHODOLOGY

The aim of this research was to find the most influential factors affecting the human component in adopting ISA in order to find a starting point to propose a theoretical ISA model for public sector employees in Oman. We began with used referenced databases to search for ISA-related articles through ScienceDirect, AISeL, SpringerLink, IEEEXplore, and Google Scholar by using keywords such as 'security awareness', 'personnel information security', 'ISA models', 'security behaviour', and awareness with all possible parameters .Due to the research scope, relevant articles published from 2010 to 2019 were identified, focusing on studies that have proposed or developed models for ISA, the human component factors of utilising psychological theories, and have been empirically tested . However, a total of twenty-one studies were considered according to their relevance to the research scope, five of which were surveys showing the level of ISA among end-users and identifying deficiencies in compliance with information security policies.

After reviewing objectives and findings of adopted studies in this paper, weight analysis was computed between an independent (IV) and dependent (DV) variable, in order to determine the relationship between them and to determine the most success predictors. Weight analysis is a computational method by which the strength of an IV is tested in order to evaluate the predictive power of the IV in a certain relationship [11]. The predictor is classified as 'well-utilised' when it has been examined five or more times and the relationships are also classified as important five or more times. The weight analysis process can be done firstly, by counting the number of times the pair of variables are examined. Secondly by counting the number of times that the relationship between the pair itself is significant, and lastly by dividing the second value by the first value (example from Table III, Subjective Norms on Intention, Weight=5/5= 1). As a result, a weight 1 denotes that the relationship between a pair of variables is significant over all studies, while weight 0 denotes that the relationship is non-significant over all examined studies [11].

Due to the paucity of relevant articles and research constraints, we considered that the IV examined three or more times where the relationship is classified as significant for three or more times as 'well-utilised' predictors for this study, provided that the weight analysis is not less than 0.80. The 'Promising' predictors are those examined two or more times, with a weight analysis not less than 0.60, and significant relationships not less two across all sixteen studies examined.

IV. END USER AWARENESS OF INFORMATION SECURITY

Organisations consider their employees an organisational asset that should be given more care and attention. However, they perceive that their employees may be the main source of security threats and breaches [12]. Despite the efforts of various institutions to promote ISA among their employees, there are still employees who are unaware of information security requirements, even among end users [13].

The annual survey of the Department for Digital, Culture, Media and Sport- UK (DCMS) [14] reported that cyber-related fraud is considered the most common breach faced by employees of companies and charities, which had the most reported security violations.

The report of PriceWaterhouseCoopers (PwC) [14] confirmed that about 75% of large organisations and 31% of small organizations have suffered security breaches related to employees' behaviour. The same report pointed out that employee-related security breaches have increased in one year to 58% in large organisations and 22% for small organisations, indicating that staff-related security breaches are increasing and there is a growing problem. Additionally, 72% of both kinds of companies suffered employee-related breaches due to poor understanding of security policies.

Ernst & Young Global Limited's (EY) annual Global Information Security Survey and technical report [15] showed that, through the previous surveys, staff were seen as the most likely source of an attack, where 57% of organisations supported the same opinion. In the same context, 38% considered unaware employees as the potential threat. In contrast, and four years later, the EY's annual Global Information Security Survey [16] reported that 34% of organisations still see unaware or careless employees as the biggest vulnerability to information security risks.

In an explorative study, [17] investigated levels of employees' awareness in one Australian organisation, showing that a lot of organisations' end users are still unaware of information security importance. The results were in terms of employee behaviours: 52.9% of participants have given passwords or logged somebody onto a computer by using their own password; 77.3% have left their work computer unlocked; 34.1% used unsuitable methods for storing their passwords; and 74% have clicked on unknown email links. Surprisingly, more than half of staff is unaware of their organisation's information security policy. Table I summarizes the above studies that have concluded that there is a weakness in the level of ISA even among end-users, which is due to a defect in security awareness programs in addition to employees' negligence and carelessness.

Table- I: Studies Indicate a Lack of End Users' ISA

Type of study	Findings	Reference
Annual survey	• The most common breaches were cyber-related fraud directed and targeted to employees. • These common breaches are considered one of the most reported breaches.	[13].
Annual survey	• 75% of large organisations and 31% of small organisations have suffered of security breaches related to employees' behaviour. • There was an increase in employees' related security breaches over one year, to 58% in large organisations and 22% for small organisations. • 72% of companies suffered employee-related breaches due to poor understanding of security policies.	[14].
Annual survey	• 57% of participating organisations supported that the staff are the most potential source of an attack. • 38% considered unaware employees as the potential threat.	[15].
	• 34% of organisations still see that unaware or careless employees as the biggest vulnerability to information security risks.	[16]
Explorative study to examine employees' awareness in an Australian organization	• 52.9% of participants have given passwords or logged somebody onto a computer by using their own password. • 77.3% of participants have left their work computer unlocked. • 34.1% used unsuitable method for storing their passwords. • 74% have clicked on unknown email links. • More than a half of staff is unaware about their organisation's information security policy.	[17].

V. REVIEW OF PREVIOUS ISA MODELS & UTILISED PSYCHOLOGICAL THEORIES

Various frameworks and models which are fully or partly linked to a particular aspect of ISA rising were identified. These sixteen models and frameworks are listed in Table II, along with study objective, utilised theory and variables.

In an empirical study of how to encourage users to protect themselves from any potential security risks and threats, Mamonov and Benbunan-Fich [18] drew on the perspective of the Information Processing (IP) framework, which assumes that mitigating threats usually occurs before full cognitive assessment of a threat. However, the results indicated that self-efficacy did not interact with any of the behavioural threat reduction strategies. Wahyudiwan, Sucahyo, and Gandhi [19] considered that ISA is temporal, so an institution should periodically measure employees' security awareness and provide appropriate improvement programmes. Depending on the core variables: knowledge, Attitude, and Behaviour of the KAB model, they measured the level of ISA for an institution's employees using seven focus areas of information security (IS). The relationships of the study's hypotheses empirically proved that knowledge has an effective impact on attitude and behaviour; in addition, attitude has good impact on behaviour.Based on the use of psychological theories in ISA, Han [20] presented a theoretical model to investigate the users' ISA in a bring your own device (BYOD) programmes. The proposed model utilised constructs of protection motivation theory (PMT) and general deterrence theory (GDT), because the author believes these constructs will have strong implications for security practices in raising users' ISA, although the study did not test them empirically.

Constructs of PMT have been empirically tested by Hanus and Wu [21], and findings revealed that ISA significantly affects response efficacy, perceived severity, response cost and self-efficacy, while only response efficacy and self-efficacy significantly impact actual security behaviour. Torten, Reaiche, and Boyle [22] utilised the same model as [21] but with a larger sample of diversified IT professionals and the findings of the latter were all positive without exception. Safa, and Von Solms [23] argued that knowledge sharing has an important role in the field of IS as a result of its effective and positive effects in raising employees' ISA and mitigating the risk of IS breaches. They applied their model based on the Motivation Theory (MT), Theory of Planned Behaviour (TPB) and the Triandis model. The results of all hypotheses testing were supported except self-worth satisfaction towards attitude, as the study also demonstrated that constructs of TPB and MT can be considered as success factors in raising ISA. Studies of [24], [25], and [26] utilised full or partial constructs of the TPB and PMT theories. The hypotheses results of [24] all were supported except perceived behavioural control towards users' behaviour. In contrast to [25]'s study, relationships of response cost and perceived severity towards behavioural intention were not supported. The outcomes of [26]'s study were also supported, except the construct perceived severity of PMT, and organisational narcissist and locus of control were not supported. Similarly, Gundu and Flowerday [27] concluded that behavioural intentions of employees can be affected by ISA levels. They practiced the theory of reasoned action (TRA), PMT and the behaviourism theory (BT) in order to develop behavioural intention model to improve positive security behaviours through the ISA process. However, it can be noted that an increase in knowledge makes a positive difference in attitude and behaviour. Hovav and D'Arcy [28] surveyed two different nations to examine whether national culture affected the deterrent capabilities of security awareness programmes, security policies, and computer monitoring based on GDT and advances in the deterrence literature and found that perceived certainty of sanctions and perceived severity of sanctions were significant for both samples. In a similar vein, researchers [29] utilised a deterrence pattern of GDT along with constructs from PMT, TRA and diffusion of innovation (DOI) theory to understand the reasons why some employees are not complying with security policies. Emphasising the impact of deterrence factors, Gundu [30] explained that employees behave securely when they dread the consequences. The study of Mani, Mubarak, and Choo [31] employed the SECI model, which is based on organisational knowledge creation theory (OKCT), to examine how real estate business employees gain and understand information security. Al-Omari, El-Gayar, and Deokar [32] have drawn on TPB as a theoretical basis to investigate the role of security knowledge and self-learning in shaping users' attitudes to comply with information security policies. The results showed that general ISA and technology awareness have a significant positive influence on both users' attitudes and self-efficacy towards intention to comply in addition to subjective norms. In another study, [33] saw that examining the role of ISA in enhancing compliance with security policies is a good measure of predicting employee commitment to information security.

Table- II: Related Work of ISA Utilised Factors & Theories

Author	Study Objective	Constructs	Utilised Theory/ Model
[18]	Examine how to encourage technology users to be protected from potential security threats	Privacy Self-efficacy, Awareness of IS Threats, Password Strength, and Refusal to Disclose Information	IP Framework
[19]	Measuring the level of ISA for employees of an organisation to prevent or reduce further adverse effects	Knowledge, Attitude, Behaviour	KAB Model
[20]	Investigation of the effective factors of a user's ISA	Perceived Severity of Threats, Perceived Susceptibility of Threats, Perceived Severity of Sanctions, Perceived Certainty of Sanctions, Security Technology Awareness, Cyber-security Inertia, and Perceived Recovery Cost	PMT – GDT
[21]	Study the impact of ISA on desktop security behaviour	Threat Awareness, Countermeasure Awareness, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, and Response Cost	PMT
[22]	Investigate the relationship between awareness's threat and countermeasure on compliance of IT professionals.	Threat Awareness, Countermeasure Awareness, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Response Cost, and Desktop Security	PMT
[23]	Propose a model to show how knowledge sharing of IS reduces the risk of IS incidents	Curiosity Satisfaction, Self-Worth Satisfaction, Earning Reputation, Gaining Promotion, Attitude, Perceived Behavioural Control, Subjective Norms, Intention, Organisational Support, and Trust	MT – TPB - Triandis Model
[24]	Propose a model to minimise users' behaviour risk towards information security threats	ISA, IS organizational policy, IS experience and involvement, Attitude, Subjective norms, Perceived behavioral control, Threat appraisal, Self-efficacy.	TPB - PMT
[25]	Propose and validate new model to understanding information security policy compliance depending on the persuasive psychological theories	Attitude, Subjective Norms, Self-Efficacy, Response Cost, Response Efficacy, Perceived Severity, and Perceived Vulnerability	TPB - PMT

[26]	Develop a model to investigate the understanding of assurance of information and awareness of users	Attitude, Subjective Norms, Perceived Behavioural Control, Intended Behaviour, Actual Behaviour, Organisational Narcissism, Perceived Vulnerability, Perceived Severity, Locus of Control, and Self-Efficacy	TPB – Threat Control Model, based on PMT.
[27]	Improve positive security behaviours through the ISA process	Subjective Norms, Attitude, Perceived Vulnerability, Perceived Severity, Response Efficacy, Response Cost, Self-Efficacy, Classical Conditioning, and Operant Conditioning	TRA – PMT - BT
[28]	Explore whether culture has affected the deterrent capabilities of security awareness, policies, and computer monitoring and its effectiveness in deterring IS misuse	Procedural Countermeasures, Technical Countermeasures, Moral Beliefs, Perceived Certainty of Sanctions, and Perceived Severity of Sanctions	GDT - IS deterrence literature
[29]	Propose a model to investigate why some employees do not comply with information security policies	Normative Beliefs, Threat Appraisal, Self-Efficacy, Response Efficacy, Visibility, Deterrence, and Rewards	TRA – PMT – GDT - DOI
[30]	Propose a model to enhance cyber security policy compliance among organisation's employees	Knowledge, Deterrence (Certainty &Severity), Attitude, Subjective Norm, Perceived Behavioural Control, Intention, and Behaviour	GDT - TPB
[31]	Examine how employees of real estate business gain and understand information security	Socialisation, Externalisation, Internalisation, and Combination	Nonaka's SECI Model (derived from OKCT)
[32]	Propose a model on TPB to explain users' intention to comply with information security policies and investigate the role of ISA	General ISA, Technology Awareness, Attitude, Self-Efficacy, Subjective Norms, and Intention to Comply	TPB
[33]	Developing a measurement tool to predict compliance of employees depending on examining role of ISA in enhancing them	Subjective Norms, Self-Efficacy, Controllability, IS, Security Policy, SETA Programme, Computer Monitoring, Perceived Usefulness of Protection, Perceived Ease of Use, and Intention	External variables – TAM constructs

VI. FINDINGS AND DISCUSSION

Despite the diligent efforts of various organisations to promote awareness of information security to their staff, the reviewed surveys and explorative studies (Table I) indicate that there is a lack of security awareness even among end users. In order for those in charge of education, training and awareness programmes to overcome this shortcoming, identifying the factors that influence ISA is a priority. Figure 1 shows all used constructs and their relationships, which were investigated to raise ISA among employees.

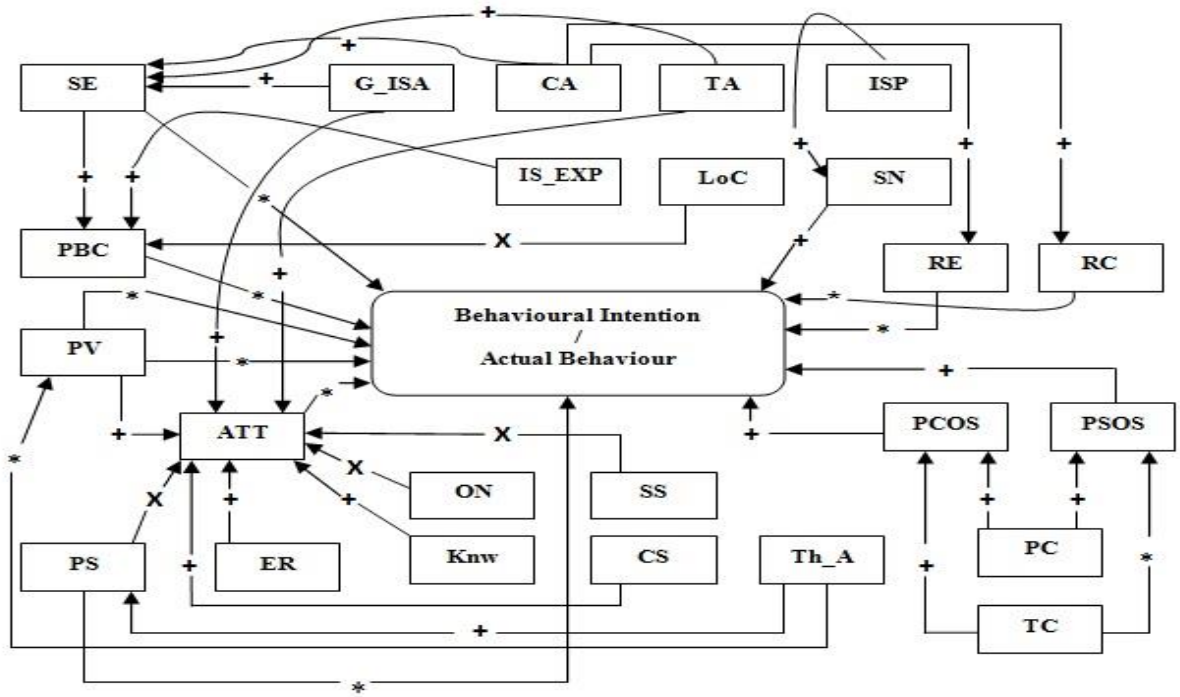

Fig. 1: ISA Constructs & Relationships Among them.

ATT: Attitude; PS: Perceived Severity; PV: Perceived Vulnerability; ER: Earning Reputation; ON: Organisational Narcissist; Knw: Knowledge; SS: Self-Satisfaction; CS: Curiosity Satisfaction; Th_A: Threat Awareness; TC: Technical Countermeasures; PC: Procedural Countermeasures; PCOS: Perceived Certainty of Sanction; PSOS: Perceived Severity of Sanction; RE: Response Efficacy; RC: Response Cost; SE: Self-Efficacy; PBC: Perceived Behavioural Control; G_ISA: General Information Security Awareness; CA: Countermeasures Awareness; TA: Technical Awareness; ISP: Information Security Policy; IS_EXP: Information Security Experience; LoC: Locus of Control; SN: Subjective Norms. +: Significant; x: Non-Significant; *: Mixed Relationships.

Our analysis of previous work related to ISA shows that the DV's intention is most utilised (thirty-one significant relationships out of thirty-seven across the sixteen studies) accompanied by subjective norms, attitude, self-efficacy and perceived vulnerability. For IVs that have been tested three or more times and whose relationships are classified as significant for three or more times and their weight analysis is equal to 0.80 or more, including subjective norms, attitude, perceived vulnerability, and self-efficacy. Moreover, there are IVs that have been tested three times but whose weight analysis is less than 0.80, more than 0.60, and have a significant relationship for only twice, such as perceived severity, and response efficacy. Table III presents the most utilised relationships between the IV and DV, the number of significant (SIG) and not significant (NS) relationships, weight analysis, and variable classification.

Table- III: Most Utilised Relationships & Weight Analysis, (Approach adapted from [11])

IV	DV	SIG	NS	Total	Weigh	Classification
Attitude	Intention	4	1	5	0.80	Well-utilised
Subjective Norms	Intention	5	0	5	1	Well-utilised
Self-Efficacy	Actual Behaviour	2	2	4	0.50	-
Self-Efficacy	Intention	3	0	3	1	Well-utilised
Attitude	Actual Behaviour	3	0	3	1	Well-utilised
Perceived Vulnerability	Intention	3	0	3	1	Well-utilised
Perceived Vulnerability	Actual Behaviour	2	1	3	0.66	Promising
Perceived Severity	Intention	2	1	3	0.66	Promising
Perceived Severity	Actual Behaviour	2	1	3	0.66	Promising
Response Efficacy	Intention	2	1	3	0.66	Promising
Intention	Actual Behaviour	3	0	3	1	Well-utilised
ISA	Attitude	2	0	2	1	Promising
Subjective Norms	Actual Behaviour	2	0	2	1	Promising
Response Efficacy	Actual Behaviour	2	0	2	1	Promising
Perceived Certainty of Sanctions	Intention	2	0	2	1	Promising
Technical Countermeasures	Perceived Certainty of Sanctions	2	0	2	1	Promising
Perceived Severity of Sanctions	Intention	2	0	2	1	Promising

The weight analysis for the most -used relationships in this study indicates that the following predictors which classified as well-utilised (tested three or more times and had three or more significant relationships throughout the sixteen investigated studies), such as subjective norms on intention, (number of tests =5, number of significant tests =5), attitude on intention (number of tests =5, number of significant tests =4), self-efficacy on intention (number of tests =3, number of significant tests =3), attitude on actual behaviour (number of tests =3, number of significant tests =3), perceived vulnerability on intention (number of tests =3, number of significant tests =3), intention on actual behaviour (number of tests =3, number of significant tests =3) . The rest of the predictors in Table III can be classified as promising, but they need further examination. Thus, researchers are encouraged to expand the research scope and investigate these predictors in future studies in order to qualify them as well-utilised predictors.

Figure 2 presents an inclusive model of ISA relationships between variables, with an indication of their weight analysis, in a concise form of what was presented in Figure 1 and Table III.

Furthermore, analysis of the results for this study shows that the constructs of PMT and TPB are the most utilised variables to propose and develop models related to the ISA domain. This is because these two models offer a good pattern for control, prediction and motivation, and the models' survey instruments have been widely validated. From the results of studies that focus on deterrence factors, we found that all relationships between predictors of GDT and behavioural intention or actual behaviour were classified as significant relationships, despite few tests (two times). Therefore, we believe that these predictors are may help overcome some cultural differences that are prevalent in the world, especially the Gulf Cooperation Council (GCC) countries, that lead to information security breaches such as nepotism, carelessness, and fear of losing face [34], where the constructs of GDT such as (Perceived severity of sanctions and Perceived certainty of sanctions) based on rational decision-making and control criminal behaviour in humans and make them comply with information security policies, [35].

Some studies utilised factors based on related literature, where these facilitate the conditions to obtain the desired behavioural intentions or actual behaviour. Therefore, we think conditions such communication, trust and organisational support need to be explored and tested in the context of ISA in order to ensure that they actually make an action easy to take.

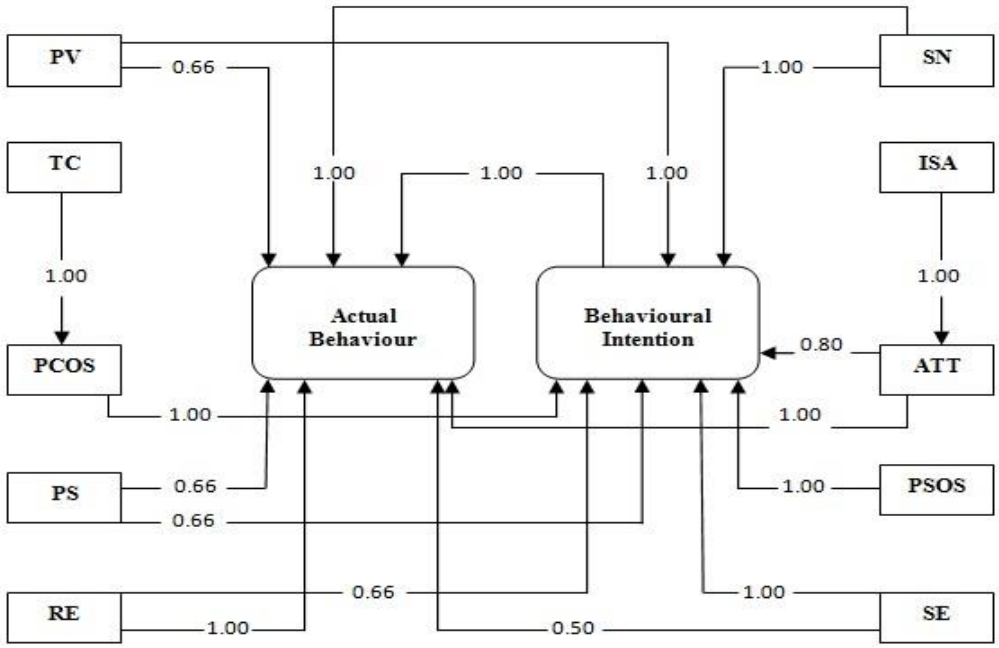

Fig. 2: Weight Analysis of Most Used Relationships in ISA.

ATT: Attitude; PS: Perceived Severity; RE: Response Efficacy; PV: Perceived Vulnerability; TC: Technical Countermeasures; PCOS: Perceived Certainty of Sanction; PSOS: Perceived Severity of Sanction; SE: Self-Efficacy; ISA: Information Security Awareness; SN: Subjective Norms.

VII. CONCLUSION & FUTURE WORK

Overall, the findings of the first five surveys stated that the defect in full employee commitment to follow information security policies is a failure to understand those policies as required, in addition carelessness and indifference. To overcome this issue, those responsible for security awareness campaigns and training programmes must employ the most successful factors in raising ISA among employees. The purpose of reviewing the other sixteen empirical studies was to identify the most commonly utilised construct relationships in raising ISA and highlight the variables of success. Emphasis was placed on relevant studies published during this decade which included models, psychological theories, and frameworks. Furthermore, out of sixteen investigated studies, the seventeen most commonly used relationships of IV and DV were extracted and investigated. Out of seventeen investigated relationships, six IVs were found to be classified as 'well-utilised' variables with a weight analysis greater than or equal to 0.80. Moreover, the rest of the IVs converged at the 'Promising' classification level; six were examined only two times but with a weight of 1 and no negative relationship. Four were examined only three times but with a weight of 0.66 and one negative relationship. In general, relying on the most successful factors in raising awareness of information security is a step in the right direction. Therefore, we expect that employing the findings of this study in our future work will lead to positive results as the weight analysis is an appropriate approach to determine the most successful factors.

The limitations of this study are concentrated in the research scope and technique used. Weight analysis was used as the sole parameter in the classification of factors influencing ISA among employees. Due to the paucity of relevant, published studies in the current decade, the research scope can be extended to include relevant published articles from the past decade, undertake meta-analysis, and adopt more statistical methods to provide an inclusive picture of predictor performance. Moreover, future studies can concentrate extensively on additional factors that affect ISA instead of focusing on psychological theories' core constructs. This study provides an initial starting point by determining the factors influencing ISA when it comes to making a decision to select those factors. Our future research plans to propose and validate the ISA model using the findings of this study, in order to enhance the ISA process in Oman.

REFERENCES

1. Internet World Stats. Middle East Internet Usage & Population Statistics [Internet]. 2019 (cited 2019Oct 30). Available from: https://www.internetworldstats.com/stats5.htm.
2. Global Data. Oman's Cards and Payments Industry: Emerging Opportunities, Trends, Size, Drivers, Strategies, Products and Competitive Landscape. [Internet]. 2015 (cited 2019 Apr 30). Available from: https://www.globaldata.com/store/report/vr1025mr--omans-cards-and-payments-industry-emerging-opportunities-trends-size-drivers-strategies-products-and-competitive-landscape/.
3. ITA. Information Technology Authority Annual Report 2017. [Internet]. 2018 (cited 2019 Nov 1) Available from: https://www.ita.gov.om/ITAPortal/Data/English/DocLibrary/FID2018516151341644/ITA%20Annual%20Report%202017.pdf
4. Ramalingam R, Lakshminarayanan R, Khan S. Information Security Awareness at Oman Educational Institutions: An Academic Prespective. arXiv preprint arXiv:1605.05580. 2016 May 17.
5. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly. 2010 Sep 1; 34(3):523-48.
6. Hagen JM, Albrechtsen E, Hovden J. Implementation and effectiveness of organizational information security measures. Information Management & Computer Security. 2008 Oct 10.
7. Hargreaves C, Prince D. Understanding Cyber Criminals and Measuring Their Future Activity, Lancaster University. [Internet]. 2013 (cited 2019 Mar 11).Available from: http://eprints.lancs.ac.uk/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf
8. Smith A, Papadaki M, Furnell SM. Improving awareness of social engineering attacks. In IFIP World Conference on Information Security Education 2009 Jul 27 (pp. 249-256). Springer, Berlin, Heidelberg.
9. Dinesh Nair. Bank Muscat says to recover pre-paid card fraud amount. [Internet]. 2013 (cited 2018 Sept 12). Available from: https://www.reuters.com/article/oman-bankmuscat/bank-muscat-says-to-recover-pre-paid-card-fraud-amount-idUSL5N0JG01A20131201
10. Al Shaibany, S. Cybercrime on the rise in Oman. [Internet].2017 (cited 2018 Sep 13). Available from: https://www.thenational.ae/world/cybercrime-on-the-rise-in-oman-1.60488
11. Rana NP, Dwivedi YK, Williams MD. A meta-analysis of existing research on citizen adoption of e-government. Information Systems Frontiers. 2015 Jun 1; 17(3):547-63.
12. Nostro N, Ceccarelli A, Bondavalli A, Brancati F. Insider threat assessment: A model-based methodology. ACM SIGOPS Operating Systems Review. 2014 Dec 5; 48(2):3-12.
13. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security. 2014 May 1; 42:165-76.
14. PriceWaterhouseCoopers PwC. INFORMATION SECURITY BREACHES SURVEY 2015 [Internet]. 2015 (cited 2019 Oct 13). Available from: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf
15. The EY's Global Information Security. Get ahead of cybercrime EY's Global Information Security Survey 2014 [Internet]. 2014 (cited 2019 Oct 15). Available from: https://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf
16. The EY's Global Information Security. Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19 [Internet]. 2018 (cited 2019 Oct 15). Available from: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
17. Chan H, Mubarak S. Significance of information security awareness in the higher education sector. International Journal of Computer Applications. 2012 Jan 1; 60(10).
18. Mamonov S, Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. Computers in Human Behavior. 2018 Jun 1; 83:32-44.
19. Wahyudiwan DD, Sucahyo YG, Gandhi A. Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education. In2017 3rd International Conference on Science in Information Technology (ICSITech) 2017 Oct 25 (pp. 654-658). IEEE.
20. Han B. User's Information Security Awareness in BYOD Programs: A Theoretical Model. Paper presented at the Information Institute Conference, Las Vegas, NV. 2017 (cited 2019 Oct 06). Available from: http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_HAN.pdf
21. Hanus B, Wu YA. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Information Systems Management. 2016 Jan 2; 33(1):2-16.
22. Torten R, Reaiche C, Boyle S. The impact of security awareness on information technology professionals' behavior. Computers & Security. 2018 Nov 1; 79:68-79.
23. Safa NS, Von Solms R. An information security knowledge sharing model in organizations. Computers in Human Behavior. 2016 Apr 1; 57:442-51.
24. Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behaviour formation in organizations. Computers & Security. 2015 Sep 1; 53:65-78.
25. 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.
26. Cox J. Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior. 2012 Sep 1; 28(5):1849-58.
27. Gundu T, Flowerday SV. Ignorance to awareness: Towards an information security awareness process. SAIEE Africa Research Journal. 2013 Jun; 104(2):69-79.
28. 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 Mar 1; 49(2):99-110.
29. Siponen M, Pahnila S, Mahmood MA. Compliance with information security policies: An empirical investigation. Computer. 2010 Feb 8; 43(2):64-71.
30. Gundu T. Acknowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance. In ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019 2019 Feb 28 (p. 94). Academic Conferences and publishing limited.
31. Mani D, Mubarak S, Choo KK. Understanding the Information Security Awareness Process in Real Estate Organizations Using the SECI Model. In20th Americas Conference on Information Systems (AMCIS 2014) 2014 Aug 1 (pp. 7-10).
32. Al-Omari A, El-Gayar O, Deokar A. Information security policy compliance: the role of information security awareness. In: K. D. Joshi and Youngjin Yoo, editors. 18th Americas Conference on Information Systems 2012, AMCIS 2012.Vol 2. 2012. Association for Information Systems. p. 1633–40.
33. Al-Omari A, El-Gayar O, Deokar A. Security policy compliance: User acceptance perspective. In2012 45th Hawaii International Conference on System Sciences 2012 Jan 4 (pp. 3317-3326). IEEE.
34. Alkahtani HK. Raising the information security awareness level in Saudi Arabian organizations through and effective, culturally aware information security framework. [Internet]. 2018 (cited 2019 Apr 30). Available from: https://dspace.lboro.ac.uk/2134/28120
35. Lebek B, Uffen J, Neumann M, Hohler B, H. Breitner M. Information security awareness and behavior: a theory-based literature review. Management Research Review. 2014 Nov 11; 37(12):1049-92.

AUTHORS PROFILE

Mr. Issam Al-Shanfari is PhD student at UTeM University Malaysia. He previously was a student of National College of Science and Technology which is affiliated with the University of Westminster - UK from 1999 to 2002 and graduated with a High National Diploma in computing. From 2003 to 2004 he was a student of Dhofar University and obtained Bachelor of computer science. He works as a computer technician for the ministry of education in Oman from 2003 until now. He studied Master at University Science Islam Malaysia (USIM) majoring in Computer Science / Information Security and Assurance (ISA) 2015.

Dr. Warusia Mohamed Yassin is a senior lecturer in Department of Computer Systems and Communication at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM). He is a member of information security, digital forensic and computer networking (INSFORNET) research group. He completes his Bachelor Degree in Computer Science (2008), Master of Science (2011) and PhD (2015) at Universiti Putra Malaysia (UPM). His research interests include Security in Computing, Machine Learning and Cloud Computing.

Dr. Raihana Syahirah Abdullah is a senior lecturer in Department of Computer Systems and Communication at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM). She is a member of information security, digital forensic and computer networking (INSFORNET) research group. She completes her Bachelor Degree in Computer Networking, Master of Computer Science, and PhD in Network Security at (UTeM). Her research interests include Computer and Network Security, Botnets, Malware Analysis.