IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 24, 2021, accepted August 19, 2021, date of publication August 24, 2021, date of current version September 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3107426

Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression

HUI NA CHUA[1], (Senior Member, IEEE), JIA SHENG TEH[2], AND ANTHONY HERBLAND[3]

[1]Department of Computing and Information Systems, Sunway University, Selangor 46150, Malaysia
[2]Department of Risk Advisory, Deloitte Business Advisory Sdn Bhd, Kuala Lumpur 60000, Malaysia
[3]School of Health and Social Work, University of Hertfordshire, Hatfield, Hertfordshire AL10 9AB, UK

Corresponding author: Hui Na Chua (huinac@sunway.edu.my)

This research was supported by the Ministry of Education Malaysia Fundamental Research Grant Scheme [FRGS/1/2019/ICT04/SYUC/02/2].

This work involved human subjects in its research. Approval of all ethical and experimental procedures and protocols was granted by the Sunway University Research Ethics Committee under Application No. SUREC 2020/074.

ABSTRACT The technological evolution has formed new challenges for organizations to safeguard their information as digital assets. Information Security Awareness (ISA) is the cognitive state where individuals comprehend information security, threats, and the capability to develop preventive strategies. Prior studies discovered that human mistakes or misbehavior is the most vulnerable link in information security due to insufficient security awareness. There were massive data breaches reported throughout the years globally. Literature shows that individuals will develop their evaluations of risks and sense of security awareness when receiving security risk information such as data breach incidents. These indications motivated us to examine the effect of an unexplored factor, that is, data breach publicity (DBR) on ISA. The purpose of this research is to discover if DBR significantly improves a model's ability to predict ISA and its magnitude in influencing ISA. A 3-stage hierarchical linear regression approach was used to build up the model with prior known influential factors to predict ISA. To the extent of our knowledge, there is no study reported to date regarding the implication of DBR on ISA. Our main findings reveal that DBR significantly explains 6.7% of ISA and achieves the highest coefficient comparing with prior known factors. Our research contributes to a novel discovery of a new factor that significantly influences ISA and its magnitude in increasing ISA. This discovery implies the need to incorporate the knowledge of data breach incidents into ISA-related educative programs or strategies to increase ISA.

INDEX TERMS Data breach publicity, hierarchical regression, information security awareness, information privacy.

I. INTRODUCTION

As organizations in this era heavily rely on Information Systems (IS) to function and ensure high productivity, the concern for information security has emerged as one of the top priorities in any organization's security management [1], [2] to maintain information availability [3], confidentiality and integrity [4]. As a result, information security issues have become a concern for most businesses, as they would result in severe consequences, for instance, corporate liability, financial loss, reputation, and credibility damage [5]. To minimize the security risks, organizations have deployed technical measures such as implementing security technologies to safeguard business information assets [6]. Nonetheless, it was found that investing in such technologies solely is inadequate to eliminate security risks and is not fully adequate to guarantee information security [7].

Researchers asserted that the weakest link in the information security system is usually due to the employees' misused behavior; more specifically, employees' naïve mistakes and accidental or intentional harm are the most prevalent factors leading to security breaches [4], [8].

Information Security Awareness (ISA) is important as it would significantly impact employees' security behavior and

The associate editor coordinating the review of this manuscript and approving it for publication was Zhitao Guan.

their adherence to the organization's security policies and regulations [9]. ISA can be denoted as an individual's cognition whereby he or she processes information regarding information security, which can be described by understanding the essentialness of information security and developing consciousness and awareness on security objectives, issues, vulnerabilities; and possessing interest towards acquiring the necessary skill sets and knowledge to utilize information systems responsibly [10].

Findings from several pieces of research demonstrated that the primary cause of information system misuse behavior and its repercussions among employees is insufficient security awareness regarding Information Security Policies (ISP) and security best practices [11]. Although previous literature has extensively presented the significance of employees' ISA, several investigations showed that ISA is still a crucial subject to comprehend. Most employees in the organizations do not possess adequate ISA on security incidents, regulations, and policies [12].

In Malaysia, the Personal Data Protection Act 2010 (PDPA) is enforced to safeguard individuals' data, but it does not have obligations for notification if a data breach occurs in an organization. In prior studies, organizations' practices and policy implementation for ensuring personal data security were found inadequate [13]. A massive data breach from Malaysian local Telco companies was first discovered that there was a leak of information on phone numbers and personal information for more than 46 million users. Nonetheless, the leak was estimated to have happened between 2012 and 2013, and there were at least 178 cases of data breaches reported until 2019 [14]. Internationally, some of the high-profile data breaches that happen throughout the years involve large corporations. [15], [16].

Work in [17] showed that individuals would develop and form their subjective perceptions and evaluations of risks when they receive news about these risks, making these risks more prominent in an individual's mind. A prior study in [18] further supported that a security breach can immediately develop an individual's perception of vulnerability and susceptibility to risks and harms. Literature [19] also revealed that the frequency of data breach news dissemination affects data protection awareness.

Previous studies have focused on different perspectives such as architectures of security awareness programs, initiatives, and strategies [20] for predicting ISA. The known factors studied by prior works and found significantly affecting ISA [11], [21] include information security policy, ISA knowledge, training, negative experience, media influence, peer behavior, and culture. Further, prior studies indicated that when an individual recognizes a threat through reading security-related publications [45], it will develop a sense of awareness [37] and negative experience [46]. This reasoning will indirectly enable them to pay more attention to information security.

Nonetheless, to the extent of our knowledge, no scientific study reported thus far has examined the implication of data breach publicity on ISA. As such, our research seeks to answer the following:

RQ1) Does DBR have a significant influence in improving a model's ability to predict ISA?
RQ2) How does DBR affect ISA?

Answering these research questions provides novel evidence to discover if a new factor (DBR) can significantly improve a model's ability to predict ISA and its magnitude in affecting ISA. This evidence will lead to the implication if there is a need to incorporate data breach incidents into an ISA educative program or strategy for improving ISA.

The rationale for choosing hierarchy regression modelling as the primary approach is based on its capability in enabling more than one variable (i.e., factor) to be added into a predictive model in separate stages called ''blocks'' to statistically ''control'' for certain variables, to investigate whether adding a predictor variable(s) (i.e., the DBR) significantly improves the model's ability to predict the target variable (i.e., ISA). Further, hierarchy regression also allows the analysis of the DBR effect on ISA through observing the regression coefficients (β). The regression coefficient represents the mean change in the target variable (i.e., ISA) for one unit of change in the predictor variable (i.e., DBR) while holding other variables in the model constant. These capabilities suit the context of our research questions setting in RQ1 and RQ2, respectively. Our approach of using hierarchy regression contributes to a methodological demonstration of how this approach can be applied in a similar research scenario.

II. LITERATURE REVIEW

A. INFORMATION SECURITY AWARENESS (ISA)

The term ''Information Security Awareness'' (ISA) denotes an individual's passive engagement and involvement with the increased attention and interest towards security issues, concurrently developing a sense of security awareness [65] and stimulating security behaviors [22].

Parsons *et al.* [4] stated that the focus on ISA comprises of two crucial constructs:

i) The first constituent is the degree of employees' understanding concerning information security behaviors on their organization's information security policies and provisions, regulations, and guidelines [4], [23]. According to Kruger and Kearney [24], they asserted the first aspect as the extent to which the employees realize and understand the core value of information security, the hierarchy of information security that applies to the organization, and lastly, employees' initiative and abilities to ensure information security. However, Sasse and Flechais [25] argued that there are still many employees not fully comprehend what measures should be implemented and practiced in protecting information security as the knowledge derived from information security policies and guiding principles might not be thorough for employees to develop a more profound comprehension on securing information assets truly.

ii) The second element in describing ISA pertains to the degree to which employees' motivation, commitment, and behavior reflect on the organization's core information security mission, in line with meeting the prerequisites for information security best practices [4], [23].

Bulgurcu *et al.* [23] also categorized ISA as two different components, which are General Information Security Awareness (GISA) and Information Security Policy Awareness (ISPA), respectively. GISA is described as an individual's general comprehension and knowledge of information security issues and threats, whereas ISPA is an employee's knowledge and comprehension to meet and achieve the organization's information security policy prerequisites. Thereupon, exploring and understanding the concept of ISA, factors influencing ISA are imperative to develop practical security knowledge and consciousness to mitigate security risks.

Researchers in the information technology domain have presented different approaches to investigate ISA [13], [26]. For example, studies on exploring information security awareness on social media were conducted. Apart from that, Stanton *et al.* [27] examined ISA by performing a survey to study security behaviors on password settings. Moreover, studies investigating smartphone users' ISA were also conducted [28].

ISA is not a behavior factor, but it usually leads to developing and cultivating security behavior [9], [30]. On the contrary, security behavior is built up based on behavioral theories such as General Deterrence Theory, Protection Motivation Theory, and Theory of Planned Behavior that affect an individual's behavior to safeguard information security, for instance, an individual's intention to conform with information security policies [6].

B. RELATED STUDIES OF INFLUENTIAL FACTORS (KNOWN FACTORS) ON ISA

Literature has shown that ISA positively affects security policy compliance behavior [12], [31]. Therefore, it is crucial to identify influential factors that significantly impact ISA. Prior studies discovered numerous influential factors. They are: i) information security policies, ii) Security, Education, Training and Awareness (SETA) programs, iii) information system knowledge, iv) negative experience of security incidents, v) media influence, vi) peer behavior, v) organizational culture and information security culture. Each of these factors is discussed as follows.

Establishing Information Security Policies (ISPs) is essential in an organization's information security management [32]. ISP is referred to as a ''direction-giving document'' [33] for employees to follow and adhere to the organization's regulations [33]. Several scholars described ISPs as a plethora of roles, responsibilities, regulations, and guidelines that are stipulated to safeguard an organization's crucial digital assets, resources, and information technology [34], [35]. Previous studies have proven that ISP provisions that are accessible and understandable positively impact an individual's ISA and knowledge [29].

SETA is a program that aims to educate and train employees to develop their information security principles awareness and potential risks to an organization's valuable assets [36]. SETA programs encompass a wide range of different approaches, methods, and measures that involve implementing security education, training, and awareness-raising activities [36], [37]. Prior researches have contended that the reinforcement and implementation of SETA programs have helped to reduce and discourage user's misuse and risky security behavior, subsequently lowering the information security-related errors caused by employees [22], [34], [38]. Findings presented in prior studies revealed that security training carried out in organizations strongly influences employees' ISA to the cognitive and behavioral extent [32], [39] that help to increase employee's ISA substantially through the inculcation of security knowledge. Several pieces of research have also suggested different methods, such as employee involvement [40], discussion, and phishing training [41] that helped raise ISA. Security education helps to form employees' interest and consciousness about security issues, thereby raising awareness and helping them to develop preventive measures on the organization's vulnerability to security threats [42].

The term ''IS Knowledge'' is often referred to as the comprehensive understanding of an information system encompassing a broad range of components, including computer knowledge, self-efficacy, and innovativeness with computing technology [43]. Kruger *et al.* [3] asserted that an individual's ability to protect and enhance integrity, confidentiality and information availability is based on understanding the constructs of information security, which indeed IS knowledge is necessary. For example, to prevent security incidents from happening, it is vital to understand the consequences that virus infection may result from an individual's careless security behavior when using the Internet, using strong passwords to protect personal information, and practicing regular backups to recover from a loss caused by security threats [44]. There are prior studies [30], [37] that empirically have proven that an individual's degree of IS knowledge has a positive association with ISA.

Individuals might have encountered different security incidents in their lives due to misbehavior and carelessness when handling information. Security incidents may happen in numerous forms. For example, individuals themselves might experience passwords being stolen, accounts being hacked, credit card fraud, or even fall for a phishing mail when using the Internet. Additionally, they might also gain security experiences from their peers, family members and through reading security-related news articles [45]. These personal experiences might be a valuable lesson for developing a sense of awareness [37]. It can be deduced that when individuals have a better overall understanding of security incidents, they will be more careful and warier in terms of cognition and behavior in ensuring information security [45]. Furthermore,

individuals must recognize that it will lead to negative implications [46]. Consequently, this cognitive reasoning will indirectly enable them to pay more attention to it.

Spreading security awareness involves more than providing security education and establishing security policies. Hence, the critical factor is that it must be accessible and reachable to its audience. Happer and Philo [47] proclaimed that the mass media has supported developing and shaping public understanding, which also leads to the essential change in behavior. The media landscape has tremendously evolved and transformed over the years [48]. Social media, as one of the communication mediums, is progressively superseding traditional media [49]. In the business context, a prior study showed that social media marketing positively impacts raising awareness and buying behavior [50]. However, there is scant research attention devoted to exploring social media's impact on awareness in the information security domain despite other application fields that presented concrete evidence that social media impact an individual's awareness.

Behavioral literature has demonstrated the importance of subjective norms, which indicates that the perceptions of individuals considered significant to an employee influence how the employee behaves [51]. It is found that employees tend to adhere to an organization's security policies if they notice that people around them, particularly managers, supervisors, colleagues, and subordinates, are also fulfilling their responsibilities in adhering to security provisions and regulations [32]. The literature claimed that if those deemed an important person to the employee in advocating and supporting the employee to adhere to the organization's security regulations, the employee will follow their advice [32]. Prior studies also denoted that the expectations of an employee's peers indirectly form a persuasive pressure and influence on his or her positive security adherence attitude, and this attitude will also derive a significant impact on other employees [51], [52]. Prior studies also showed that employees develop security awareness through conversation and discussion with their peers [39], [40].

Information security culture relates to the implemented measures and employees' behavior to protect the organization's digital assets [53]. Research has also revealed that solid leadership support has an extensive impact on information security management and the cultivation of a better security culture [54]. Literature also claimed that security culture is strongly associated with the organization's mission and vision [55]. Several pieces of research have made significant contributions to the association between organizational culture and information security culture [2], [56], [57]. Connolly *et al.* [58] had proven that organizations that focus more on employee interaction and culture tend to have a positive direction towards ISA. Several studies have also implicated that information security culture notably influences an individual's ISA [56], [59]. Parsons *et al.* [60] found that employees who are more knowledgeable and aware of information security issues tend to conform with established policies when an organization has a robust and vigilant security culture. Wiley *et al.*'s [61] findings further confirmed that security culture plays a role as a mediator between the association of ISA and organization culture.

C. DATA BREACH PUBLICITY

A data breach is a security incident, which involves unauthorized access, disclosure, usage, or disposal of data, often personal data [62]. A data breach may lead to illegal access or exposure of confidential, sensitive, or any protected information that encompasses personally identifiable information, health-related information, trade secrets, or intellectual property [63]. Data breaches can happen in different ranges of scopes, from impacting a few persons to a large group of customers [63].

Some of the high-profile data breaches that happen throughout the years involve large corporations such as Facebook, Yahoo, Equifax, and Marriot. For example, in 2018, Facebook reported that around 87 million users' data had been inappropriately harvested by Cambridge Analytica [15]. Apart from that, in 2018, Marriott International, an American multinational hospitality organization that operates a large group of hotels, revealed that records from 500 million guests were breached and stolen by an unauthorized party on its hotel reservation systems [16].

Martin *et al.* [18] argued that a security breach is capable of immediately developing an individual's perception of vulnerability and susceptibility to risks and harms. Kahneman [17] showed that individuals would develop and form their subjective perceptions and evaluations of risks when they receive information from the news regarding these risks, making these risks more prominent in an individual's mind. Additionally, data breach information dissemination frequency was found to impact data protection awareness [19] significantly.

Despite the potential of data breach publicity on ISA, as far as we know, there are no studies reported that have empirically proven how DBR can improve a model's ability to predict ISA.

III. METHODOLOGY

A. STUDY DESIGN

For data collection, an online survey questionnaire was formulated according to the factors we wanted to include in the hierarchical regression model for testing, including the demographic and known factors studied by literature, and the new factor, DBR, that we are interested in investigating.

Known factors of ISA were adopted based on previous literature as the research framework, except for the Data Breach Publicity factor, which was proposed for investigation in this study. The survey instruments were adopted and adapted from several previous works of literature [23], [29], [39], [61], [64]–[71].

The scale for the target variable, i.e., ISA, was adopted based on Bulgurcu *et al.*'s [23] research dimensions of GISA, which measures the employee's general information

security knowledge and comprehension. All the factors were measured using four items and employing a 5-point Likert scale ranging from 'Strongly Disagree' (1) to 'Strongly Agree' (5).

A survey test run was also carried out before officially rolling out the survey. A total of 8 respondents were involved in the test run to provide their suggestions and opinion regarding the survey questionnaire. The distribution of their age group falls between 20 to 50 years old across different ethnicities. In addition, the respondents come from different working backgrounds, such as three respondents were reported from Banking and Finance fields, two were working in the Food and Beverage field, and the other three were from Telecommunications field.

Several refinements were done based on the test run from the respondents' opinions and recommendations; for instance, the working industries were expanded to cover a few other prominent working fields, such as service and healthcare. Furthermore, to avoid confusion when reading ''other platforms'' as compared to social media platforms to stimulate awareness on information security in one of the questions, the ''other platforms'' terms were changed to ''TV/radio/newspapers''. Apart from that, other comments stated that the questionnaire is well-designed and understandable.

The questionnaire was distributed and managed from June to August 2020, using Google Forms, to examine individual's Information Security Awareness (ISA). Participants were not required to have an email or Google account to access the Google Forms distributed. The survey was done through a snowball sampling approach. Respondents were recruited from invitations through social media platforms and email solicitations. The responses were kept private and confidential to assure the respondents' anonymity. The respondents were requested to provide their demographic characteristics comprising of their age, ethnicity, gender, and employment by industry sector.

To serve as validation, approval for the study and the overall research procedure was obtained from the Sunway University Research Ethics Committee (Reference No.: SUREC 2020/074).

B. MODELLING AND ANALYSIS DESIGN

We performed a 3-stage hierarchical regression analysis to determine if DBR significantly improves a model's ability to predict ISA and its magnitude in influencing ISA by considering all other known factors (i.e., demographic and known factors). As contrasted with multivariate linear regression, this hierarchical approach was assessed by testing the change in R-square (R^2) from one stage to the next. We built three regression models in three stages using this model comparison framework by adding previously known ISA factors studied by prior literature, i.e., demographic and known factors, as variables to a preceding model in each stage.

Our interest in this study is to conclude whether the newly added variable, i.e., DBR, significantly improves explaining ISA. The R^2 indicates the proportion of variance in ISA, which DBR accounts for in the final stage of the multiple regression analysis [75]. The first stage model (Model in Stage-1) includes demographic information such as age, gender, ethnicity, and the working industry. In the next stage (Model in Stage-2), we added and replicated known variables (namely the prior studied influential ISA factors discussed in Section II-B) reported by previous research. In the final stage (Model in Stage-3), we added the variable of DBR that we are interested in to answer if DBR can significantly improve a model's ability to predict ISA by considering all other known factors. The 3-stage hierarchical regression model is presented as follows:

$$\begin{aligned}
&\text{Model in Stage-1:}\\
&\quad \text{ISA} = \text{Intercept_1} + \text{demographic variables}\\
&\text{Model in Stage-2:}\\
&\quad \text{ISA} = \text{Intercept_2} + \text{demographic variables}\\
&\qquad + \text{known ISA variables}\\
&\text{Model in Stage-3:}\\
&\quad \text{ISA} = \text{Intercept_3} + \text{demographic variables}\\
&\qquad + \text{known ISA variables} + \text{DBR} \qquad (1)
\end{aligned}$$

Because our first research question (RQ1) aims to answer if DBR can significantly improve a model's ability to predict ISA, in other words, our interest is to determine if the final Model in Stage-3 explains ISA better than Model in Stage-2. If there is a statistically significant difference of R^2 between Model 2 and 3 (i.e., R^2 change), it can be concluded that the added DBR explains ISA beyond the demographic and known factors in Model Stage-2. Our first research question (RQ1) can be answered by referring to this conclusion. Therefore, we do not consider the options of entering DBR into Stage-1 or Stage-2 models without considering the demographic and known ISA factors. The significance level for the model procedures was set to $p < 0.05$

For answering our second research question (RQ2) of how DBR affects ISA, we will observe the coefficient (β) of DBR in the Stage-3 model. The coefficient (β) indicates how much ISA is expected to increase when the DBR variable increases by one, holding all the demographic and known variables constant.

IV. RESULTS

A. DATA COLLECTED

Table 1 presents the demographics of respondents. A total collection of 529 responses were gathered in this survey. The gender population was considered equal, comprising 263 (49.7%) male and 266 (50.3%) female respondents. The age distribution for the respondents ranges from below 21 years to 51 years old and above.

The respondents' mean and standard deviation (SD) age were 36.7 and 11.0, respectively, showing a considerably balanced distribution whereby there was no age group dominating the sample. Similarly, with the occupation factor, we

observed no dominance among the industries. We observed that most of our respondents were Malaysian Malay and Malaysian Chinese, which totaled 413 respondents (78.1%), followed by Malaysian Indians. As there was no data available showing specifically the population distribution between the age of 18 years old and above from the Malaysian Statistics Department, it was unfeasible to derive and confirm the statistical significance of the racial balance in the ratio of the Malaysian population.

Based on the multigroup analysis on the ISA score in Table 1, the '21-30' years old respondents were the most aware of information security (ISA mean = 4.30). Female respondents scored higher ISA than males (4.18). The Malay ethnicity respondents were the most information security-aware (4.39). The respondents working in the Banking & Finance industry scored the highest ISA with a mean score of 4.42 compared to other industries, followed by the Telecommunication and Information Technology industries.

TABLE 1. Demographics of respondents.

Descriptions	Sample Size (N = 529)		ISA score
	n	%	mean (SD)
Age			
Below 21	6	1.1	3.92 (0.46)
21-30	190	35.9	4.30 (0.55)
31-40	158	29.9	4.20 (0.63)
41-50	94	17.8	4.25 (0.52)
51 and above	81	15.3	4.09 (0.65)
Gender			
Male	263	49.7	4.18 (0.60)
Female	266	50.3	4.27 (0.57)
Ethnicity			
Malay	186	35.2	4.39 (0.52)
Chinese	227	42.9	4.12 (0.58)
Indian	98	18.5	4.18 (0.67)
Others	18	3.4	4.19 (0.46)
Working Experience			
1-5 years	127	24.0	4.27 (0.54)
6-10 years	128	24.2	4.28 (0.59)
11-15 years	80	15.1	4.13 (0.63)
16-20 years	57	10.8	4.34 (0.60)
21 years and above	137	25.9	4.13 (0.59)
Industry			
Information Technology	74	14.0	4.41 (0.46)
Service	73	13.8	4.07 (0.67)
Others	73	13.8	4.14 (0.55)
Banking & Finance	69	13.0	4.42 (0.49)
Food & Beverages	65	12.3	4.14 (0.59)
Healthcare	41	7.8	4.34 (0.56)
Property & Development	36	6.8	4.04 (0.61)
Telecommunications	32	6.0	4.41 (0.48)
Education	31	5.9	4.08 (0.68)
Manufacturing	27	5.1	4.14 (0.55)
Energy (Oil/Gas)	8	1.5	4.38 (0.60)

B. VALIDITY AND RELIABILITY

Table 2 represents the questionnaire instruments utilized to evaluate each item with their respective loadings, average variance extracted (AVE), and Composite Reliability (CR). All the item loadings were significant, in which all the constructs do not fall below 0.7, the recommended minimum cut-off value [74].

The AVE value measures variation captured by a factor as a construct concerning the amount of variation due to measurement error. Finally, the value of CR is a measure of internal consistency in scale questionnaire items. Moreover, reliability and internal consistency validation were also performed for the latent variables based on Cronbach's Alpha scores with the minimum threshold cut-off value of 0.7.

The CR assessment scores indicated that the items met the prerequisites of accounting good reliability and were well-developed. Results also demonstrated that the AVE values exceeded the suggested threshold of 0.50 [70]. Therefore, we fully adopted or partially adapted questionnaire items of ISA, ISP, SETA, ISK, NEX, SMI, PEB, ORC, and SEC listed from prior studies presented in Section III-B.

For the Data Breach publicity factor as a new construct, we developed the questionnaire items as follows:

DBR1: The publicity of data breach incidents allows me to be aware of the potential risks and consequences if the information is not appropriately protected.

DBR2: The publicity of data breach incidents draws my attention to implement necessary security measures to protect my information.

DBR3: Sharing publicized data breach incidents with my families and friends is important to help them increase information security awareness.

DBR4: It is essential for the relevant authorities to increase the publicity of data breach incidents timely to reduce financial loss in individuals and organizations.

C. PRELIMINARY ANALYSES

Preliminary analyses were performed to confirm there was no violation of the four assumptions of linear regression [72], which are: i) normality (to determine if our sample is well-modelled by a normal distribution), ii) linearity (to check if there is a relationship between a factor variable and ISA significantly without bias), iii) multicollinearity (to confirm there are no factor variables that are too highly correlated with each other), and iv) homoscedasticity (to ensure a condition in which the variance (or error) in our regression model does not vary much as the value of the factor variables change, in other words, the spread of the errors is constant across the modelling process.). Except for a multicollinearity violation between age and working experience, no other significant violations were encountered. Hence

parametric tests were conducted. Consequently, the 'working experience' variable was discarded for the subsequent analyses.

D. CORRELATION ANALYSIS

We performed correlation analyses to identify the strength of the linear relationship between the main factor variables. Table 3 presents the correlation matrix, which examines the relationship between ISA, ethnicity (ENC), age (AGE), gender (GEN), industry (IDT), ISP, SETA, ISK, NEX, SMI, PEB, ORC, SEC, and DBR. Because a correlation matrix is symmetrical, only half of the correlation matrix is displayed. As there are no highly correlated variables (correlation coefficient ≥ 0.8) with each other in the model, we ruled out the potential multicollinearity problem.

1) ISA AND DEMOGRAPHIC FACTORS

Referring to Table 3, there is inconclusive evidence about the significance of the association between ISA and Ethnicity and Gender because their effects did not achieve statistical significance ($p < 0.05$). While the relationship between ISA and age was statistically significant, the small magnitude of -0.09 indicates the association between ISA and age is trivial, practically not correlated. On the contrary, the correlation between ISA and industry is 0.16, implying little association between the two. The Kruskal-Wallis H test was performed to gain a better insight into the association between ISA and industry. Based on the test results, there was a divergence in the respondents' ISA across different industries. We observed respondents from industry sectors of ICT (Information Technology and Telecommunications) and Banking & Finance (mean scores of both sectors = 4.4) were likely to have higher ISA, followed by Healthcare (mean score = 4.3), compared to other sectors (mean scores ranging from 4.0-4.1).

2) ISA AND NON-DEMOGRAPHIC FACTORS

There were significant associations between ISA and other non-demographic factor variables, with the magnitude of correlation coefficients between 0.5 and 0.7 (that is, Table 3 cells highlighted in grey), suggesting that those variables can be considered moderately positively correlated. In addition, it is found that the data breach publicity (DBR) posed the strongest strength in the relationship with ISA significantly, compared to all other variables. This observation indicates a strong positive association between ISA and DBR.

E. HIERARCHICAL REGRESSION MODELLING

A summarized 3-stage hierarchical regression is presented in Table 4. The 3-stage hierarchical regression was applied to examine the extent to which factor variables predicted ISA. The summarized table also presents the estimates for the parameters encompassed in the final predictive model. The coefficients (β) of the final regression model Stage-3 described the relationship of each studied factor held against ISA mean score, while all other variables are kept constant.

TABLE 2. Item measurement and loadings, CR and AVE.

Items	Questions	Loading	CR	AVE
ISA	Information Security Awareness (partially adopted from [23])			
	ISA1	0.826	0.870	0.627
	ISA2	0.757		
	ISA3	0.812		
	ISA4	0.770		
ISP	Information Security Policy (adapted from [65] [66])			
	ISP1	0.700	0.826	0.543
	ISP2	0.739		
	ISP3	0.743		
	ISP4	0.763		
SETA	Security, Education, Training & Awareness (adapted from [34])			
	SETA1	0.831	0.908	0.712
	SETA2	0.882		
	SETA3	0.831		
	SETA4	0.829		
ISK	Information Systems Knowledge (adapted from [69])			
	ISK1	0.816	0.866	0.618
	ISK2	0.811		
	ISK3	0.766		
	ISK4	0.749		
NEX	Negative Experience (partially adapted from [68])			
	NEX1	0.772	0.861	0.608
	NEX2	0.779		
	NEX3	0.789		
	NEX4	0.778		
SMI	Social Media Influence (adapted from [64])			
	SMI1	0.708	0.839	0.566
	SMI2	0.820		
	SMI3	0.751		
	SMI4	0.725		
PEB	Peer Behavior (adopted from [65])			
	PEB1	0.757	0.851	0.587
	PEB2	0.787		
	PEB3	0.779		
	PEB4	0.742		
ORC	Organizational Culture (adapted from [71])			
	ORC1	0.770	0.859	0.603
	ORC2	0.771		
	ORC3	0.773		
	ORC4	0.792		
SEC	Security Culture (adopted from [65])			
	SEC1	0.700	0.845	0.578
	SEC2	0.807		
	SEC3	0.770		
	SEC4	0.760		
DBR	Data Breach Publicity			
	DBR1	0.719	0.857	0.600
	DBR2	0.796		
	DBR3	0.781		
	DBR4	0.800		

The effects of demographics information, discovered by prior studies to predict ISA [61], [73], were tested at Stage 1. Our results on the demographics information model were statistically significant ($p = 0.001$) but only explained 2.7% of the variation of ISA. As highlighted in prior

TABLE 3. Correlation matrix: gender, age, ethnicity, industry, ISA, ISP, SETA, ISK, NEX, SMI, PEB, ORC, SEC, and DBR.

	ISA	ENC	AGE	GDR	IDT	ISP	SETA	ISK	NEX	SMI	PEB	ORC	SEC
ENC	0.07												
AGE	-.09*	-0.13**											
GDR	0.07	0.13**	0.03										
IDT	0.16**	0.20**	-0.18**	0.04									
ISP	0.65**	0.02	-0.08	0.09*	0.17**								
SETA	0.57**	0.04	-0.14**	-0.03	0.19**	0.62**							
ISK	0.58**	0.09*	-0.22**	-0.02	0.23**	0.56**	0.63**						
NEX	0.60**	-0.01	-0.002	0.04	0.16**	0.54**	0.47**	0.47**					
SMI	0.63**	0.15**	-0.19**	0.03	0.20**	0.59**	0.55**	0.62**	0.61**				
PEB	0.60**	0.06	-0.09*	-0.01	0.17**	0.67**	0.77**	0.64**	0.50**	0.63**			
ORC	0.58**	0.12**	-0.23**	0.01	0.21**	0.64**	0.64**	0.59**	0.46**	0.60**	0.72**		
SEC	0.72**	0.05	-0.12**	0.03	0.16**	0.70**	0.70**	0.61**	0.55**	0.61**	0.72**	0.66**	
DBR	0.75**	0.06	-0.09*	0.14**	0.09*	0.67**	0.44**	0.49**	0.61**	0.57**	0.54**	0.59**	0.64**

Note: *p < 0.05; **p < 0.001

TABLE 4. Summary of the hierarchical regression analysis.

Variables	Cumulative			Simultaneous (the final model in Stage-3)	
	Adjusted R^2-change	F-change	*p* value-change	Coefficient (β)	*p*-value
Entered at Stage-1	0.027	F(4, 524) = 4.6	0.001		
Ethnicity				0.012	0.652
Age				0.028	0.289
Gender				-0.001	0.977
Industry				0.018	0.499
Entered at Stage-2	0.588	F(8, 516) = 100.1	< 0.001		
ISP				0.016	0.686
SETA				0.091	0.036
ISK				0.092	0.012
NEX				0.075	0.035
SMI				0.120	0.002
PEB				-0.030	0.525
ORC				-0.038	0.348
SEC				0.254	<.0001
Entered at Stage-3	0.067	F(1, 515) = 111.4	< 0.001		
DBR				0.413	<0.001

literature [23], [34], [64]–[66], [68], [69], the effect of previously reported factors (namely ISP, SETA, ISK, NEX, SMI, PEB, ORC, SEC) as known factor variables were entered at Stage 2, and it was found that they collectively explained an additional 58.8% of the variation in ISA.

Data Breach Publicity (DBR) was hypothesized as a sub-component of ISA, and it was entered at Stage 3. The result shows that it explains an additional 6.7% of the variation in ISA. The final regression model accounted for a total of 68.2% variance (R^2) in ISA. The F-change with a significance of $p < 0.001$ means that data breach publicity added in Model Stage-3 significantly improved the ISA prediction.

In Table 4, the β values and p values represent the results of the final complete model in Stage-3. The coefficient (β) of DBR achieves the highest score of 0.413 compared with other

known factors. This finding indicates that one unit change of DBR will significantly ($p < 0.001$) affect 0.413 times the mean change in ISA while holding other variables in the model constant. Remarkably, regardless of the initial significant correlation with ISA, the Age (AGE), Industry (IDT), Information Security Policy (ISP), Peer Behavior (PEB), and Organizational Culture (ORC) were insignificant ($p > 0.05$) covariates in the final regression model.

V. DISCUSSION

Not reported in prior studies, our main finding confirmed and answered this study's first research question (RQ1) that data breach publicity is a significant factor for improving a model's ability to predict ISA by observing the positive increment of R^2 change in the hierarchical regression model. Furthermore, after controlling for demographic factors and other prior studies reported factors, data breach publicity predicted an additional 6.7% of ISA variability in the hierarchical regression analysis.

The DBR achieves the highest coefficient (β) with a positive 0.413, comparing with prior known factors. Hence, we can infer that data breach publicity has the highest positive effect on ISA than prior known factors. This finding answered our second research question (RQ2).

Contradictory to previous literature findings by Schlienger and Teufel [59] and Da Veiga *et al.* [56], as indicated in our final model, organizational culture was an insignificant factor, though security culture showed otherwise. However, these findings align with the recent study of Wiley *et al.* [61] that explained a more compound association between ISA, security culture, and organization culture, where security culture poses a mediator role in the relationship between ISA and organization culture. Furthermore, the correlation analysis in our study also confirmed the association between ISA, security culture, and organization culture. This finding implies that regardless of organizational culture, better security culture is possibly a stronger predictor of an individual's ISA.

Significant relationships between ISA and factors of negative experience, information systems knowledge, and SETA were found in the final model. Similar results were reported by Haeussinger & Kranz [29] and Mani *et al.* [39]. On the other hand, the model analysis shows no significant relationship between ISA and peer behavior, which is inconsistent with previous research that stated employees develop security awareness through conversation and discussion with their peers [39], [40]. Further examination is required to investigate the interplay of peer behavior influence with other factors, especially the socio-environmental antecedents of ISA, to understand this contradiction.

Also, no significant relationship was found between ISA and security policy provision in the final model. This finding contradicts prior studies that suggested that information security policy provisions positively impact an individual's ISA. Organizations in Malaysia are devoting less emphasis to promoting the cruciality of information security policies in their respective organizations, which is a significant cause of why most employees are unaware of their company's security policies [12]. Without a well-established and informed security policy, employees may not be able to implement robust security measures that could help evaluate and identify potential weaknesses of information security [13].

Prior research findings [29], [39] revealed the significant effect of information obtained from traditional media on ISA. However, there is inadequate research attention dedicated to exploring the influence of social media on ISA despite other application fields presenting evidence of social media's impact on individual's awareness [50], and this communication medium is gradually replacing traditional media [49]. Our finding confirms the significant relationship between ISA and social media influence.

Our study shows that demographic factors were not significant covariates in the final hierarchical model based on our hierarchical analysis. However, compared with previous research conducted in a different country [61], a significant relationship was found between ISA, age, and gender. Thus, the variation in national characteristics between different countries may affect the relationship between ISA and demographic factors. However, the validity of this proposition needs further investigation to confirm.

A. CONTRIBUTION AND IMPLICATIONS

The results of our study encompass both theoretical and practical implications. From the aspect of theoretical implications, our findings contribute to the theoretical research work by presenting empirical evidence and confirming the association between ISA and data breach publicity, which has not been reported in the study of ISA theoretically or empirically.

We discovered a significant positive association between data breach publicity (DBR) and ISA. Essentially, individuals with the knowledge of data breach incidents were likely to have higher ISA. This finding revealed that DBR is a significant predictor and possesses the highest effect in shaping an individual's ISA. By increasing the efforts of publicizing data breach incidents, individuals are inclined to learn from these experiences and eventually develop a stronger sense of protection and vulnerability to online harms [17], [18]. Therefore, relevant authorities such as governments and media corporations should stress their role in increasing data breach incidents' publicity.

According to our research findings, security information derived from social media was discovered to carry a significant effect on an individual's awareness of information security. Thus, our findings show that social media is an effective and potent tool in building information security awareness. Moreover, because of the rapid evolution of technology, people today tend to engage and spend more time on social media. This evidence is crucial from a practical perspective. As a result, government and organizations would be more efficiently utilizing social media to disseminate data

breach incidents that would be more widespread and quicker for individuals to obtain the latest information.

This study presents a significant contribution to information security literature. The results of our study can be applied in a future investigation to examine other related factors and the effects of their interplay. For instance, it is perhaps practically useful to discover the association between DBR and other known factors relevant to information dissemination, for example, media influence, SETA, and how it may impact the perception of an individual's negative experience. More prominently, our findings also present a practical contribution. Government and industrial organizations can rely on empirical evidence to guide their strategy in disseminating information security newscasts, including data breach publicity through an effective medium such as social media.

This study also contributes to a practical exemplar case of how a 3-stage hierarchical regression approach can confirm if a newly studied factor has a significant impact in improving a predictive model's ability and how the new factor impacts the prediction. Finally, using hierarchy regression provides a methodological demonstration of how this approach can be applied in a similar research scenario.

B. LIMITATIONS AND FUTURE WORK

Our research encompasses several limitations. First, the data collection approach of our research was geographically constrained to Malaysia. Henceforth, to populate the findings, future researchers should consider the study in other countries and regions, where cultural variation might be an external factor that yields a distinct perspective on findings. Second, one of the plans to extend this study is collecting randomized sample data with more balanced demographics and dimensions.

Moreover, the present research does not explore the interlinking effects that each influential factor possesses. Therefore, future research should consider investigating the effects between the factors affecting ISA, as these predictors might have intertwined impacts when affecting an individual's ISA.

Another avenue for future work is that researchers could examine the effects of data breach publicity on influencing an individual's information privacy and security compliant behavior since the proposed factor was a relatively new finding in the field. Besides, demographic characteristics of different data samples might reflect divergence in findings. For example, the correlation analysis of our study shows respondents from different industries posed different levels of ISA. Therefore, a future study may be conducted with a larger data sample to analyze different industry sectors.

VI. CONCLUSION

Our research provides novel evidence that data breach publicity has a significant positive impact on a model's ability to predict ISA, and it also demonstrates the highest positive effect on ISA compared to prior known factors. Relevant authorities such as governments and media corporations should stress their role to increase the publicity of data breach incidents. To improve employees' ISA, organizations should strategize their ISA programs to include data breach publicity. Using hierarchy regression contributes to a methodological demonstration of how this approach can be applied in a similar research scenario that requires empirical testing on an unknown factor's effect if it can improve a model's ability for prediction by considering prior known factors.

REFERENCES

[1] S. Ransbotham and S. Mitra, "Choice and chance: A conceptual model of paths to information security compromise," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 121–139, Mar. 2009.
[2] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, Jun. 2010.
[3] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Inf. Manage. Comput. Secur.*, vol. 18, no. 5, pp. 316–327, Nov. 2010.
[4] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.
[5] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME," in *Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Kuala Lumpur, Malaysia, Nov. 2013, pp. 286–290.
[6] S. Aurigemma, "A composite framework for behavioral compliance with information security policies," *J. Organizational End User Comput.*, vol. 25, no. 3, pp. 32–51, Jul. 2013.
[7] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Comput. Secur.*, vol. 31, no. 8, pp. 983–988, Nov. 2012.
[8] E. Schultz, "The human factor in security," *Comput. Secur.*, vol. 24, no. 6, pp. 425–426, Sep. 2005.
[9] A. Al-Omari, O. El-Gayar, and A. Deokar, "Security policy compliance: User acceptance perspective," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Honolulu, HI, USA, Jan. 2012, pp. 3317–3326.
[10] M. E. Thomson and R. von Solms, "Information security awareness: Educating your users effectively," *Inf. Manage. Comput. Secur.*, vol. 6, no. 4, pp. 167–173, Oct. 1998.
[11] S. Abraham, "Information security behavior: Factors and research directions," in *Proc. 17th Amer. Conf. Inf. Syst.*, Detroit, MI, USA, 2011, pp. 4050–4062.
[12] H. N. Chua, S. F. Wong, Y. C. Low, and Y. Chang, "Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations," *Telematics Inform.*, vol. 35, no. 6, pp. 1770–1780, 2018.
[13] M. F. Gan, H. N. Chua, and S. F. Wong, "Privacy enhancing technologies implementation: An investigation of its impact on work processes and employee perception," *Telematics Informat.*, vol. 38, pp. 13–29, May 2019.
[14] R. Yunus. (2019). *Almost 200% Increase in Data Breach Attacks Since 2018*. [Online]. Available: https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/
[15] C. Kang and S. Frenkel, "Facebook says Cambridge analytica harvested data of up to 87 million users," The New York Times, 2018. [Online]. Available: https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.htm
[16] J. Valinsky. (2018). *Marriott Reveals Data Breach of 500 Million Starwood Guests*. [Online]. Available: https://edition.cnn.com/2018/11/30/tech/marriott-hotels-hacked/index.html.
[17] D. Kahneman, *Thinking, Fast and Slow*. New York, NY, USA: Farrar, Straus and Giroux, 2011.
[18] K. D. Martin, A. Borah, and R. W. Palmatier, "Data privacy: Effects on customer and firm performance," *J. Marketing*, vol. 81, no. 1, pp. 36–58, Jan. 2017.
[19] N. W. J. Yan and H. N. Chua, "A path analysis model to identify the effects of social media, news media and data breach on data protection regulation awareness," in *Proc. IEEE 2nd Int. Conf. Artif. Intell. Eng. Technol. (IICAIET)*, Sep. 2020, pp. 1–6.
[20] M. Karjalainen and M. Siponen, "Toward a new meta-theory for designing information systems (IS) security training approaches," *J. Assoc. Inf. Syst.*, vol. 12, no. 8, pp. 518–555, Aug. 2011.

[21] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manage. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, Nov. 2014.
[22] T. R. Peltier, "Implementing an information security awareness program," *Inf. Syst. Secur.*, vol. 14, no. 2, pp. 37–48, 2005.
[23] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quart.*, vol. 34, no. 3, pp. 523–548, Sep. 2010.
[24] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, Jun. 2006.
[25] M. S. Flechais, "Usable security: Why do we need it? How do we get it?" in *Security and Usability*. Sebastopol, CA, USA: O'Reilly Media, 2005, pp. 13–30.
[26] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *Privacy Enhancing Technologies*. Berlin, Germany: Springer, 2006, pp. 36–58.
[27] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Comput. Secur.*, vol. 24, no. 2, pp. 124–133, Mar. 2005.
[28] N. Clarke, J. Symes, H. Saevanee, and S. Furnell, "Awareness of mobile device security: A survey of user's attitudes," *Int. J. Mobile Comput. Multimedia Commun.*, vol. 7, no. 1, pp. 15–31, 2016.
[29] F. Haeussinger and J. Kranz, "Information security awareness: Its antecedents and mediating effects on security compliant behavior," in *Proc. 34th Int. Conf. Inf. Syst.*, Milan, Italy, 2013, pp. 1–16.
[30] F. Hassandoust and A. A. Techatassanasoontorn, "Understanding users' information security awareness and intentions: A full nomology of protection motivation theory," in *Cyber Influence and Cognitive Threats*, 1st ed. Amsterdam, The Netherlands: Elsevier, 2018, pp. 129–143.
[31] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Inf. Manage. Comput. Secur.*, vol. 22, no. 1, pp. 42–75, 2014.
[32] M. Chan, I. Woon, and A. Kankanhalli, "Perceptions of information security in the workplace: Linking information security climate to compliant behavior," *J. Inf. Privacy Secur.*, vol. 1, no. 3, pp. 18–41, Jul. 2005.
[33] M. S. Corpuz, "The enterprise information security policy as a strategic business policy within the corporate strategic plan," in *Proc. 8th Int. Symp. Risk Manage. Cyber-Inform.*, Orlando, FL, USA, 2011, pp. 275–279.
[34] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.
[35] M. E. Whitman, "Security policy: From design to maintenance," in *Information Security: Policy, Processes, and Practices*. New York, NY, USA: M. E. Sharpe, 2008, pp. 123–151.
[36] B. Gardner, "What is a security awareness program?" in *Building an Information Security Awareness Program*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 1–8.
[37] F. Haeussinger and J. Kranz, "Antecedents of employees' information security awareness—Review, synthesis, and directions for future research," in *Proc. 25th Eur. Conf. Inf. Syst.*, Guimarães, Portugal, 2017.
[38] M. Siponen, M. A. Mahmood, and S. Pahnila, "Are employees putting your company at risk by not following information security policies?" *Commun. ACM*, vol. 52, no. 12, pp. 145–147, 2009.
[39] D. Mani, S. Mubarak, and K. K. R. Choo, "Understanding the information security awareness process in real estate organizations using the SECI model," in *Proc. 20th Americas Conf. Inf. Syst.*, Savannah, GA, USA, 2014, pp. 1–11.
[40] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Comput. Secur.*, vol. 29, no. 4, pp. 432–445, 2010.
[41] R. C. Dodge, C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *Comput. Secur.*, vol. 26, no. 1, pp. 73–80, Feb. 2007.
[42] T. Qing, B. Y. Ng, and A. Kankanhalli, "Individual's response to security messages: A decision-making perspective," in *Decision Support for Global Enterprises*, vol. 2. Boston, MA, USA: Springer, 2007, pp. 177–191.
[43] Z. Tu and Y. Yuan, "Critical success factors analysis on effective information security management: A literature review," in *Proc. 20th Americas Conf. Inf. Syst.*, Savannah, GA, USA, 2014, pp. 1–13.
[44] L. Drevin, H. A. Kruger, and T. Steyn, "Value-focused assessment of ICT security awareness in an academic environment," *Comput. Secur.*, vol. 26, no. 1, pp. 36–43, Feb. 2007.
[45] P. Zhang and X. Li, "Determinants of information security awareness: An empirical investigation in higher education," in *Proc. 36th Int. Conf. Inf. Syst.*, 2015, pp. 4321–4328.
[46] K. Aytes and T. Connolly, "A research model for investigating human behavior related to computer security," in *Proc. 9th Americas Conf. Inf. Syst.*, Tampa, FL, USA, 2003, pp. 2027–2031.
[47] C. Happer and G. Philo, "New approaches to understanding the role of the news media in the formation of public attitudes and behaviours on climate change," *Eur. J. Commun.*, vol. 31, no. 2, pp. 136–151, Apr. 2016.
[48] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," *Bus. Horizons*, vol. 52, no. 4, pp. 357–365, 2009.
[49] S. Kemp. (2019). *Digital 2019: Essential Insights Into How People Around the World Use the Internet, Mobile Devices, Social Media, and E-Commerce*. We Are Social. [Online]. Available: https://p.widencdn.net/kqy7ii/Digital2019-Report-en
[50] M. Saravanakumar and T. SuganthaLakshmi, "Social media marketing," *Life Sci. J.*, vol. 9, no. 4, pp. 4444–4451, 2012.
[51] I. Ajzen, "The theory of planned behavior," *Organizational Behav. Hum. Decis. Processes*, vol. 5, no. 2, pp. 179–211, 1991.
[52] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *Proc. 40th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2007, p. 156b.
[53] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 243–256, Apr. 2015.
[54] K. J. Knapp, T. E. Marshall, R. Kelly Rainer, and F. Nelson Ford, "Information security: Management's effect on culture and policy," *Inf. Manage. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, Jan. 2006.
[55] A. B. Ruighaver, S. B. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, Feb. 2007.
[56] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.
[57] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, Oct. 2006.
[58] L. Y. Connolly, M. Lang, J. Gathegi, and D. J. Tygar, "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study," *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 118–136, 2017.
[59] T. Schlienger and S. Teufel, "Analyzing information security culture: Increased trust by an appropriate information security culture," in *Proc. 14th Int. Workshop Database Expert Syst. Appl.*, Prague, Czech Republic, Sep. 2003, pp. 405–409.
[60] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, "The influence of organizational information security culture on information security decision making," *J. Cogn. Eng. Decis. Making*, vol. 9, no. 2, pp. 228–240, 2015.
[61] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and information security awareness," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101640.
[62] B. C. F. Choi, S. S. Kim, and Z. Jiang, "Influence of firm's recovery endeavors upon privacy breach on online customer behavior," *J. Manage. Inf. Syst.*, vol. 33, no. 3, pp. 904–933, 2016.
[63] S. Chatterjee, X. Gao, S. Sarkar, and C. Uzmanoglu, "Reacting to the scope of a data breach: The differential role of fear and anger," *J. Bus. Res.*, vol. 101, pp. 183–193, Aug. 2019.
[64] A. Kaur and H. S. Chahal, "Role of social media in increasing environmental issue awareness," *J. Arts, Sci. Commerce*, vol. 9, no. 1, pp. 19–27, 2018.
[65] A. Da Veiga, "An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture," *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 584–612, Nov. 2018.
[66] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, Apr. 2009.
[67] J. D'Arcy and A. Hovav, "Does one size fit all? Examining the differential effects of IS security countermeasures," *J. Bus. Ethics*, vol. 89, no. S1, pp. 59–71, May 2009.

[68] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, Nov. 2009.
[69] G. Bassellier, I. Benbasat, and B. H. Reich, "The influence of business managers' IT competence on championing IT," *Inf. Syst. Res.*, vol. 14, no. 4, pp. 317–336, 2003.
[70] A. Bhattacherjee and G. Premkumar, "Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test," *MIS Quart.*, vol. 28, no. 2, pp. 229–254, 2004.
[71] D. R. Denison *et al.*, "Diagnosing organizational cultures: Validating a model and method," Documento de trabajo, Denison Consulting Group, Frauenfeld, Switzerland, Tech. Rep., 2006, pp. 1–39.
[72] D. C. Montgomery, E. A. Peck, and G. G. Vining, *Introduction to Linear Regression Analysis*. Hoboken, NJ, USA: Wiley, 2021.
[73] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Comput. Hum. Behav.*, vol. 69, pp. 151–156, Apr. 2017.
[74] W. W. Chin, "Issues and opinion on structural equation modelling," *MIS Quart.*, vol. 22, no. 1, pp. 7–16, 1998.
[75] D. Cramer, "Hierarchical multiple regression," in *Advanced Quantitative Data Analysis*. London, U.K.: McGraw-Hill, 2003, ch. 6, pp. 74–85.

HUI NA CHUA (Senior Member, IEEE) received the Ph.D. degree from the University of Nottingham, U.K. She joined academia after working in the industry for more than ten years. She is currently an Associate Professor with the Department of Computing and Information Systems, Sunway University. She had contributed and managed various Malaysian national research projects, such as the FRGS and MDEC funds and industry-based funded research and development projects when/where she worked as a full-time Technical Lead and filed more than ten patents. Her research interests include applied machine learning, text analytics, data mining, data management, and information security/privacy.

JIA SHENG TEH received the Bachelor of Science degree (Hons.) in information systems (business analytics) from Sunway University and Lancaster University, U.K. He is currently a Business Analyst with Deloitte Risk Advisory, IT, and specialized assurance field. His research interests include information privacy, data mining, data modeling and visualization, and big data analysis methods.

ANTHONY HERBLAND received the Ph.D. degree from the University of Hertfordshire, U.K. He is currently an Educational Technologist and a Senior Lecturer with the University of Hertfordshire. He has published numerous articles contributing to health science, e-learning, and statistical methodology. His research interests include data analysis and statistical methods.