International Journal of Advanced Technology and Engineering Exploration, Vol 8(74)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2020.S1762116

Research Article

Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: a structural equation modeling

Siti Daleela Mohd Wahid[1], Alya Geogiana Buja[2*], Mohd Nor Hajar Hasrol Jono[2] and Azlan Abdul Aziz[2]
Faculty of Business Management, Universiti Teknologi MARA, Kampus Alor Gajah, 78000, Melaka, Malaysia[1]
Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, Kampus Jasin, 77300, Melaka, Malaysia[2]

Received: 19-September-2020; Revised: 15-January-2021; Accepted: 18-January-2021

Abstract
The advanced growth of communication technology today greatly has brought benefits in many ways, but it has indirectly led to the exposure of data privacy and safety of end users to the outsiders. Due to the Covid-19 pandemic, all citizens are required to stay at home and most of their times have been used on the internet for their leisure, study and work purposes. The massive use of internet lead to cybercriminal like scam, fraud, hacking and cyber bullying. It has been reported that the senior adult is the most affected group. Using the Information Security Awareness Model (ISACM) and the Situation Awareness Cybersecurity Education Model (SAOCE), this study aims to develop a cybersecurity awareness model that can assist the elderly from attacks in cyberspace. Methodologically, this paper is quantitative in nature and recruits 300 senior adults from age 50 until above 60 years via convenience sampling technique. We identified three factors namely organization, social and individual influencing cybersecurity awareness. The result revealed that organization factors significantly related to cybersecurity awareness with value of β=0.151, p=0.025, meanwhile for social and individual factors are found less significant to cybersecurity awareness with values β=-0.066, p=0.328 and β=0.045, p=0.463 respectively. With the development of cybersecurity awareness model, we are confident that our model can contribute to the body of knowledge within the cybersecurity context.

Keywords
Covid-19, Cybersecurity awareness, Elderly, Structural equation modelling.

1.Introduction
The advanced growth of communication technology today has brought great benefits to the people of Malaysia in many ways. One of those is the introduction of Society 5.0 concept, in which referring to smart cities which will solve future issues and challenges using digital approaches including artificial intelligence (AI), big data and Internet of Things (IoT). Big data collected by the various devices will be analysed and transformed into new type of innovation technologies by AI and will be beneficial for all levels of the community. The aim of society 5.0 is to change our lifestyle to becoming more comfortable with digital technology and its services whenever it is needed. Despite of its advantage, some problems have come into the picture.

One of the problems is cybersecurity awareness among the elderly people. It had been reported in 2017 in the UK, the risk of senior citizens being cyber fraud victims is getting higher, which predicted more than one million elderlies will be attacked by scammer through email [1].

Statistically, 8% of 75 years old and above internet users claimed that they were a victim and almost 75% of the age group said technology had exposed them to online danger although it offers many benefits [2, 3]. There are about 62,000 complaints about fraud received from senior citizens with total loss of almost $650 million, whereas tech support fraud is speeding up and the elderlies will be the majority victims [4−6]. Therefore, it is timely to create cybersecurity awareness among the elderlies. Thus, the objective of this study is to further investigate the relationship of

*Author for correspondence

the identified factors in creating the cybersecurity awareness to the elderly.

2.Literature review

The ideology of the proposed conceptual framework is derived from two prominent models which are Information Security Awareness Capability Model (ISACM) and Situation Awareness-Oriented Cybersecurity Education (SAOCE). Previous work had developed a model of ISACM based on several theories that combined the aspect of information security best practices and security awareness theory [7]. The design of ISACM comprises three key features in which all these features are according to the controls listed within ISO/IEC 27002. The first feature is awareness importance, in which people's awareness about cybersecurity control will influence the process of avoiding being a scam victim. The second key feature is the awareness capacity, which refers to a person's capability in dealing with a problem. For example, how a person is capable to understand the type, characteristic and situation of a scam activity. This understanding could influence the rate of successful scam avoidance. Finally, the awareness risk which investigated the gap between the amounts of awareness importance being bigger than the amount portrayed by a person (awareness capability). Unfortunately, this model is limited to the individual factor only whereby we develop a comprehensive model with the aim at identifying the organization and social factor concurrently.

Another advanced model is called SAOCE. This approach was explained by [8] in his research on developing a cybersecurity education curriculum for university students. The approach was based on Situation Knowledge Reference Model (SKRM) which capture the students' awareness on the cybersecurity situations. In the proposed curriculum, several hands-on lab activities that represent real-world cyber problems were introduced to bring the conceptual knowledge unit. The proposed curriculum comprises four modules: the research module, the laboratory module, the situation awareness module and the presentation module. The advantage of this approach is it has been proven beneficial for curriculum in the university which the students are able to have intensive understanding on cybersecurity background. On the other hand, this model cannot be implemented for the senior citizens awareness and education because of the complicated computer science terminologies, concepts and technical steps that are difficult to be delivered to this group of users. Thus, a simpler cybersecurity education model is needed to teach senior citizens on how to recognize cyber-attack and prevent them from being a victim. To capture all the different aspects prior to cybersecurity awareness, we proposed a research model (see *Figure 1*) that includes variables to address organizational, social and individual factors of cybersecurity awareness. Those dimensions are the most important factors in identifying cybersecurity awareness [9−11]. Therefore, we included all the dimensions in our proposed cybersecurity awareness model for the elderly.

2.1Organization factors

The Information Security Policy contains a set of rules issued by the organization that defines the principles and responsibilities necessary to protect information. In general, the aim of determining the Information Security Policy (ISPP) is as follows: to ensure business continuity, minimize security incidents, prevent unauthorized access and protect the organization's reputation. Ideally, the policy should be well formulated and understandable. Moreover, IT security representative of the organization must ensure all policies should be reachable in both soft and hardcopy to create alertness and awareness. It should be noted that a clear and understandable ISPP will impact the cybersecurity awareness [12] especially if there is a senior citizen involved as a part of the company's team.

On the other hand, awareness programs and security training are alternative ways to increase cybersecurity awareness. A responsible organization should hold training session that engage employees and ensure they comprehend the procedures and mechanisms in place to protect the information [10, 11]. It is advisable the training session should cover the broad scope from collect/use/delete data until the appropriate use of social networking. Frequent security training is needed if the company employs more senior citizens. It is a firm belief that the key to enhance the security awareness is through security training [12].

Theoretically, the security culture should reflect the information security beliefs and values that are collectively shared by all the employees at every level of an organization [12]. It is suggested that the ISC should change the employee's motivation for cyber awareness [13]. In another development, understanding the facets of information security can help all employees, especially the elderlies, in their daily work [14]. In other development, by educating every employee especially among the elderly people

on the aspects of information security can help them to perform in their daily job [14]. From the abovementioned discussion, the following hypothesis is developed:

H1: The organization factors (i.e., security training and awareness program, information security policy provision and information security culture) is positively related to cybersecurity awareness.

2.2Social factors

The social factors can be divided into "primary sources that include family members, friends or co-workers and secondary sources like the mass media" [11] and public administration [9]. These sources are particularly significant in assisting individuals especially the elderlies to minimize the cybersecurity risk involved [9]. For example, the consequences of cybersecurity incidents are not always noticeable so the word-of-mouth spreading by family and friends can enhance the learning process for cybersecurity issues.

Researches have confirmed that information that are received from multiple medium such as television, books and articles are significantly related to security behavior [15,16]. In Malaysia, campaigns on awareness had long been conducted to educate the people about cybercrime and online safety. Several departments have joined hand to promote and organize special program to support the awareness campaign. In similar fashion, [17] argues on the impact that the mass media have on the public awareness concerning information security issues. We argue that the awareness has largely increased the interest and knowledge on information security.

Public administrations play a significant role in promoting cybersecurity awareness [18,19]. Therefore, majority of the citizens will comply or oblige with the information provided by the public administrations that highlight the significance of cybersecurity and the delivery of security advices [9]. Based on the preceding discussion, the following hypothesis is developed:

H2: The social factors (i.e.., influence of mass media, family & friend and public administration) is positively related to cybersecurity awareness.

2.3Individual factors

The idea of self-initiated learning about cybersecurity topics is compulsory. We need to adjust ourselves to understand the general security actions in order to create awareness. Ironically, it is assumed that an individual who shows initiative (e.g., finds solutions to any attack problem, takes immediate countermeasures) has a positive effect on awareness [20−24]. However, for the elderly people to initiate a first-move they require strong assistance. According to [25], senior citizens have an undesirable attitude towards computers. This is due to the elderlies' dubious attitude towards the Internet, including the belief that it is unsafe, too expensive and too complex to use.

Another individual factor that requires equal exposure is the Information Security Knowledge (ISK). At this point, we are referring ISK as a general knowledge of basic application systems that are used on a daily basis. For example, an individual who knows how to open and close a document as well as able to use the copy and paste function. There is a positive relationship between the awareness of cybersecurity and computer skills [9]. Empirically, this shows that the individual's computer level (e.g., high, medium and low), knowledge of the Internet and experience has a positive influence on behavior towards security [26].

Education is another sector that requires individual's attention on cybersecurity. Being able to know, use and apply the computer system starts from school or college. In today's advanced technology, learning and practicing cybersecurity is easy. We also believe that senior adults learn a lot to adapt with the changes. Therefore, we introduced the following hypothesis:

H3: The individual factors (i.e., personal initiative, information system knowledge, security education) are positively related to cybersecurity awareness.

3.Methodology

This section presents materials and methodology of the study.

3.1Population and sample procedures

This study population consists of senior adults age 50 years old and above in Malaysia. The respondents were categorized as working, not working and retired. Selecting this group is in line with the suggestion that senior citizens are mostly at risk for any cybercrime [4−6]. Almost 75% of this age group blame technologies have made them expose to online danger. The data collection process included an online questionnaire, which was conducted via a Google form survey. Although using self-reported,

we conducted Harman's One Factor Solution analysis which allows the controlling for Common Method Variance (CMV) which was essential for this study. The data collection took place on 15 June 2020 and lasted eight weeks. The current study uses a convenience sampling technique, which refers to sampling designs that use the sample of the population that is conveniently available to provide responses [27]. The advantages of this sampling technique are quick and convenient. Previous researchers have recommended some guidelines for sample size. After examining their suggestions, we have considered 300 samples.

3.2Measurement and scaling of the theoretical constructs

In this paper, we have used two statistical software for data analysis. First, the Statistical Package for the Social Sciences (SPSS) software was used for the preliminary analysis (i.e., descriptive statistics). Later, another advanced statistics software named Analysis Moment of Structures (AMOS) was utilized to support the central analysis (i.e., Structural Equation Modelling (SEM)). The Structural Equation Modeling (SEM) "is the best multi variate procedure for testing both the construct validity and theoretical relationships." SEM is used as a more powerful approach compared to covariance analysis, path analysis, factor analysis, time series analysis, and multiple regressions [27]. By using SEM, the strength of the associations between constructs could be more accurately identified because it takes measurement errors into account.

Moreover, the SEM strategy of comparing alternative models to assess relative fit model makes it a more robust method. Nevertheless, SEM requires that several procedural steps be taken. SEM provides a conceptually engaging way to precisely test a theory regarding relationships among variables and latent constructs. In this paper, we utilized two prominent models which are Information Security Awareness Capability Model (ISACM) and Situation Awareness-Oriented Cybersecurity Education (SAOCE). When the data is presented, SEM can prove how well the theory fits [27]. Moreover, SEM produces accurate results without measurement errors. As mentioned earlier, to perform SEM, the analytical software called AMOS is used. This software is user friendly with an advanced computing engine for analysing multi-dimensional constructs which consists of multiple underlying concepts [28]. IBM AMOS software allows the analysis and testing that is fast, efficient and user-friendly. Its popularity is accredited to its descriptive ability and statistical proficiency for testing models with a single comprehensive method using various measures which reduces measurement errors and provides a better understanding of the phenomenon being studied [27].

4.Results and discussions

This section discusses the results of the study.

4.1Demographic profile

Table 1 shows the demographic profile for the senior adults who responded to the questionnaire. The 300 senior adults who took part in this survey were 56.3% (N=169) male and 43.7% (N=131) female. Most of them are 50-59 years old (59.7%, N=179), followed by above 60 years old (40.3%, N=121). In terms of race, 75.7% (N=227) are Malay, 12.3% (N=37) are Chinese, 6.0% (N=18) are Indian and 6.0% (N=18) are labelled as others. The information on the working sectors reveals that 32.3% (N=97) work at the public sectors, while 28.0% (N=84) work at the private sectors. The remaining 39.7% are from the self-employed, retired and not working group. Lastly, 49.0% (N=147) of the senior adults who are still working; work at the non-IT companies whilst, 11.3% (N=34) are working with IT companies. The 34 senior adults are more expert and advanced compared to the junior executives in the workplace in terms of securing information.

Table 1 Demographic profile

Characteristic		Frequency	Percentage
Gender	Male	169	56.3
	Female	131	43.7
Age	50-59 years old	179	59.7
	Above 60 years old	121	40.3
Race	Malay	227	75.7
	Chinese	37	12.3
	Indian	18	6.0
	Others	18	6.0

Characteristic		Frequency	Percentage
Working sector	Public	97	32.3
	Private	84	28.0
	Self-employed	40	13.3
	Retired	50	16.7
	Not working	29	9.7
Working category	IT company	34	11.3
	Non-IT company	147	49.0
	Others	119	39.7

4.2Assessment of SEM

In this section, we assessed four important elements of SEM. Firstly, we conducted the Confirmatory Factor Analysis (CFA) followed by the second element which is the measurement model. Thirdly, we tested the structural model to confirm the hypotheses development. Lastly, we executed CMV procedures through Harman's One Factor Solution analysis.

4.2.1Testing the confirmatory factor analysis (CFA)

CFA is a procedure to validate all latent variables in the model. The purpose of conducting CFA is to evaluate the fit model, the standard factor loadings, and the standard errors. The CFA is a pre-requisite for measurement models in which both the number of factor loadings and their corresponding indicators are clearly defined [29]. In CFA, the theory is proposed first, then tested to see how the constructs systematically represent latent variables [27]. There are two methods available to execute CFA: Individual-CFA and Pooled-CFA. We decided to employ the Pooled-CFA since it is more efficient, accurate and able to monitor one set of fitness indexes for all the constructs in the model. More importantly, through Pooled-CFA, it could assess the correlation between variables [30]. In the Pooled-CFA, all the constructs are assessed simultaneously. By using this method, all the constructs are grouped and linked using the double-headed arrows to evaluate the correlation among the constructs. The CFA model for four (4) latent variables ranges from 0.737 to 0.923. The model also shows that the correlation coefficients among the constructs ranges between 0.016 to 0.435, which is less than 0.900, therefore, suggesting no multicollinearity among the variables.

4.2.2Testing the measurement model

The first step of SEM is to test the measurement model. The result obtained from the Pooled-CFA process was assessed to form the measurement model. The fit indices values are Relative Chi-Square=1.626, RMSEA=0.040, CFI=0.989, TLI=0.985 and PGFI=0.596. As these fit indices meet the requirement as recommended by [27] who suggested that if three to four of the Goodness-of-Fit (GOF) indices meet the requirement, then the model is acceptable. Therefore, in this study the measurement model is declared to be a good fit. The summary of the fit model for measurement model is shown in *Table 2*. In the measurement model, we also tested the convergent validity, the construct reliability and the discriminant validity. The convergent validity refers to a set of variables or items that are assumed to measure a construct and to share a high percentage of common variance [27].

It is tested by using the factor loadings and the Average Variance Extracted (AVE). Both the factor loadings and the AVE should measure a minimum of 0.500 which indicates high convergent validity [27].

The Composite Reliability (CR) refers to the degree to which an instrument is measured according to the dimensions of the constructs [27]. The acceptable cut-off point of CR is in between 0.600 to 0.700 [27]. The overall result is presented in *Table 3*.

Table 2 Analysis for measurement model

	AFI		IFI		PFI
Fit Indices	Relative Chi Square (<5)	RMSEA (< =0.080)	CFI (> =0.900)	TLI (> =0.900)	PGFI (> =0.500)
	1.626	0.040	0.989	0.985	0.596

Notes: AFI-Absolute fit indices, IFI-Incremental fit indices, PFI-Parsimonious fit indices RMSEA- Root mean square error of approximation, CFI-Comparative fit index, TLI-Tucker-Lewis index, PGFI-parsimonious goodness of fit index

Table 3 Analysis for convergent validity and composite reliability

Constructs	Items	Factor loadings (>0.500)	AVE (>0.500)	CR
Organizational Factors (OF)	SETA	0.854	0.699	0.874
	ISPP	0.823		
	ISC	0.830		
Social Factors (SF)	MMI	0.834	0.663	0.855
	FFI	0.867		
	PAI	0.737		
Individual Factors (IF)	PI	0.905	0.790	0.919
	ISK	0.865		
	SE	0.896		
Cybersecurity Awareness (CA)	PV	0.803	0.718	0.884
	PS	0.923		
	PSE	0.810		

Notes: SETA- security training and awareness programs, ISPP- information security policy provision, ISC- information security culture, MMI- mass media influence, FFI- family & friend influence, PAI- public administration influence, PI- personal initiatives, ISK- information security knowledge, SE-security education, PV-perceived vulnerability, PS-perceived severity and PSE-perceived self-efficacy.

Meanwhile, the discriminant validity refers to "the extent to which a construct is truly distinct from other constructs" [27]. It also means that the factors or items only measure one latent construct. The threshold for AVEs is greater than 0.500. The point of discriminant validity of the constructs is to explain whether the items are redundant. Furthermore, as presented in *Table 4* by comparing the r2 values with the AVE value, the findings show that the r2 of all variables' values are less than AVEs'. Consequently, it indicates that each construct is distinct.

Table 4 Analysis for discriminant validity

Tested path			r^2	AVE_1	AVE_2	Result
⟷	OF	SF	0.189	0.699	0.663	Valid
⟷	OF	IF	0.127	0.699	0.790	Valid
⟷	OF	CA	0.019	0.699	0.718	Valid
⟷	SF	IF	0.118	0.663	0.790	Valid
⟷	SF	CA	0.000	0.663	0.718	Valid
⟷	IF	CA	0.006	0.790	0.718	Valid

Notes: OF-Organizational factors, SF-social factors, IF-individual factors, CA-cybersecurity awareness

4.2.3Testing the structural model

The second stage in SEM is to evaluate the structural model by examining the hypothesized relationships among latent variables (see *Figure 1).*

This structural model denotes one endogenous relationship linking the hypothesized model's variables. In this study, the focus of structural model is to examine and test the interrelationship between exogenous and endogenous variables. This present study adopted the Total Disaggregation Structural Model in which suggested by [27], involving only latent variables. A total of 3 hypotheses were analyzed.

The focus of testing this structural model is to examine the interrelationship between exogenous (organization, social and individual factors) and endogenous (cybersecurity awareness) variables. The results are presented in *Table 5*, showing mixed results. For OF and CA, there is a significant correlation between them, β=0.151, p=0.025. Meanwhile, the relationship between SF and CA is insignificant, β=-0.066, p=0.328. Lastly, the interplay between IF and CA also not significant, β=0.045, p=0.463.

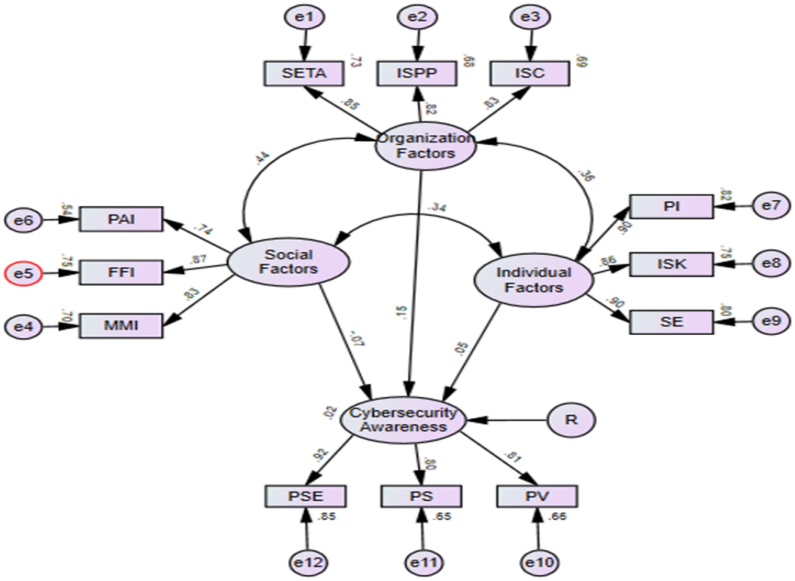

Figure 1 Structural model

Table 5 Result of hypothesis testing

H	Causal path			B	E	S.E.	C.R.	P
H_1	OF	→	CA	0.151	0.170	0.076	2.235	0.025
H_2	SF	→	CA	0.066	0.058	0.060	0.979	0.328
H_3	IF	→	CA	0.045	0.033	0.044	0.734	0.463

Notes: OF-Organizational factors, SF-social factors, IF-individual factors, CA-cybersecurity awareness

4.2.4Testing the CMV

To conduct the Harman's One Factor Solution test, CFA was performed which is a more refined analysis of the test. Two models were developed: a Harman's One Factor and a measurement model. For the Harman's One Factor, all items were loaded on one general factor. Then, the fit model of the Harman's One Factor model was compared with the fit model of the proposed measurement model.

If the Harman's One Factor model had a poor fit compared to the proposed model, then the common method variance is not present. *Table 6* shows that the goodness-of-fit indices of Harman's One Factor model have a poorer fit than the proposed measurement model. Therefore, the finding provides a confirmation that common method variance is not a problem in this study.

There are mixed findings for the personal, social and organizational determinants on an elderly. The main findings of the hypothetical path: weak to moderate social influences and personal initiative has insignificant effect. Similar to other studies with bounded limitations, this study contains some limitations too. Since this study depends on self-report data, it may contain a bias. Although the study sample displays a good balance in the gender and age items, with diversified job areas, this study discovered that most of the participants are involved in the public sector. The workplace item could effect and offer different findings, as such any future work should consider other working sectors such as the private, and the voluntary sector.

Table 6 Analysis for common method variance

	AFI		IFI		PFI
Fit Indices	Relative Chi Square (<5)	RMSEA (< =0.080)	CFI (> =0.900)	TLI (> =0.900)	PGFI (> =0.500)
Measurement Model	1.626	0.040	0.989	0.985	0.596
Harman's One Factor Solution Model	12.831	0.168	0.575	0.593	0.530

Notes: AFI-Absolute fit indices, IFI-Incremental fit indices, PFI-Parsimonious fit indices RMSEA- Root mean square error of approximation, CFI-Comparative fit index, TLI-Tucker-Lewis index, PGFI-parsimonious goodness of fit index.

5.Conclusion

This study explores the personal, social and organizational determinants of the elderly society in Malaysia. This study contributes by providing valuable insights into the research field of study in cybersecurity awareness. These insights can help to support the security practitioners in the review of security strategies to further develop and strengthen the awareness and education among the elderly society. Overall, the organization factors which consist of SETA, ISPP, ISC influence cybersecurity awareness directly. However, this study is limited to a small group of the elderly due to the short time frame. In the future, the study can be extended to the larger elderly group with longer time and extra items can be added up for the elderly that is going to be retired.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] https://eandt.theiet.org/content/articles/2017/01/the-elderly-most-at-risk-from-cyber-crime-report-warns/. Accessed 26 October 2020.
[2] Shao J, Zhang Q, Ren Y, Li X, Lin T. Why are older adults victims of fraud? current knowledge and prospects regarding older adults' vulnerability to fraud. Journal of Elder Abuse & Neglect. 2019; 31(3):225-43.
[3] König R, Seifert A, Doh M. Internet use among older Europeans: an analysis based on SHARE data. Universal Access in the Information Society. 2018; 17(3):621-33.
[4] https://cybersecurityventures.com/3-cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/. Accessed 26 October 2020.
[5] Morrison BA, Coventry L, Briggs P. Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. Frontiers in Psychology. 2020; 11:1-13.
[6] Tan SL, Vergara RG, Khan N, Khan S. Cybersecurity and privacy impact on older persons amid COVID-19: a socio-legal study in Malaysia. Asian Journal of Research in Education and Social Sciences. 2020; 2(2):72-6.
[7] Poepjes R, Lane M. An information security awareness capability model (ISACM). Australian information security management conference. 2012.
[8] Dai J. Situation awareness-oriented cybersecurity education. In frontiers in education conference 2018 (pp. 1-8). IEEE.
[9] Simonet J, Teufel S. The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users. In IFIP international conference on ICT systems security and privacy protection 2019 (pp. 194-208). Springer, Cham.
[10] D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research. 2009; 20(1):79-98.
[11] Haeussinger F, Kranz J. Information security awareness: its antecedents and mediating effects on security compliant behavior. International conference on information systems 2013.
[12] Alnatheer MA. Understanding and measuring information security culture in developing countries: case of Saudi Arabia (Doctoral Dissertation, Queensland University of Technology). 2012.
[13] Martins A, Elofe J. Information security culture. In security in the information society 2002 (pp. 203-14). Springer, Boston, MA.
[14] Alnatheer MA. A conceptual model to understand information security culture. International Journal of Social Science and Humanity. 2014; 4(2):104-7.
[15] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems. 2009; 18(2):106-25.
[16] Ng BY, Rahim M. A socio-behavioral study of home computer users' intention to practice security. PACIS Proceedings. 2005:234-47.
[17] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 2010; 34(3):523-48.
[18] Albuquerque Junior AE, Santos EM. Adoption of information security measures in public research institutes. JISTEM-Journal of Information Systems and Technology Management. 2015; 12(2):289-316.
[19] Dzazali S, Zolait AH. Assessment of information security maturity. Journal of Systems and Information Technology. 2012; 14(1):23-57.
[20] Shillair R, Dutton WH. Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. Available at SSRN 2756736. 2016.
[21] Munanga A. Cybercrime: a new and growing problem for older adults. Journal of Gerontological Nursing. 2019; 45(2):3-5.
[22] Nurse JR. Cybercrime and you: how criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624. 2018.
[23] Ricci J, Breitinger F, Baggili I. Survey results on adults and cybersecurity education. Education and Information Technologies. 2019; 24(1):231-49.
[24] Seifert A, Schelling HR. Seniors online: attitudes toward the internet and coping with everyday life. Journal of Applied Gerontology. 2018; 37(1):99-109.
[25] Wagner N, Hassanein K, Head M. Computer use by older adults: a multi-disciplinary review. Computers in Human Behavior. 2010; 26(5):870-82.
[26] Rhee HS, Kim C, Ryu YU. Self-efficacy in information security: its influence on end users'

information security practice behavior. Computers & Security. 2009; 28(8):816-26.
[27] Hair JF, Black WC, Babin BJ, Anderson RE, Tatham RL. Multivariate data analysis. Upper Saddle River, NJ: Prentice Hall.1998.
[28] Byrne BM. Structural equation modeling with AMOS: basic concepts, applications, and programming (Multivariate Applications Series). New York: Taylor & Francis Group. 2010.
[29] Kline RB. Principles and practice of structural equation modeling. Guilford Publications. 2015.
[30] Awang Z. SEM made simple: a gentle approach to learning structural equation modeling. MPWS Rich Publication. 2015.

Siti Daleela Mohd Wahid is a senior lecturer at Faculty of Business Management, Universiti Teknologi MARA, Melaka. She completed her BBA and MBA at Universiti Teknologi MARA, Malaysia. Currently, pursuing PhD under supervision of Dr Wan Mohd Hirwani Wan Hussain in social entrepreneurship at The National University of Malaysia. Her areas of interest are societal innovation, social entrepreneurship, community entrepreneurship, entrepreneurship, marketing and service quality.
Email: sitid365@uitm.edu.my

Alya Geogiana Buja is a Senior Lecturer at the Faculty of Computer and Mathematical Sciences in Universiti Teknologi MARA (UiTM) Cawangan Melaka. She is a PhD holder in the field of Information Security and graduated from Universiti Teknikal Malaysia Melaka (UTEM), MSc in Computer Science and BSc in Netcentric Computing from Universiti Teknologi MARA (UiTM). Her research interests are Networking and Information Security, Cryptanalysis and Cyber Security.
Email: geogiana@uitm.edu.my

Mohd Nor Hajar Hasrol Jono was born in 1978 in Klang, Selangor. He obtained his PhD in 2016. At present, he is working as a senior lecturer at the Faculty of Computer Science and Mathematics at Universiti Teknologi MARA (UiTM) Melaka, Malaysia. Now in the field of administration, he currently holds the position of Deputy Rector of Student Affairs UiTM Melaka. Previously, he was the Head of Training Division, Head of Systems Division and also Fellow at the i-Learn Center under the Academic Affairs Division, UiTM Shah Alam.
Email: hasrol@uitm.edu.my

Azlan Abdul Aziz is a senior lecturer at the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Melaka. From 2001 to date, he has served as Internal Auditor, Fellow and Head of Content Development Division at the i-Learn Centre, a committee in the Vice Chancellor Special Project, an innovation and competition judge, reviewer and editor. He is a PhD holder in the field of Multimedia Education and graduated from Universiti Pendidikan Sultan Idris (UPSI), Masters of Info. Tech. in Information Science and B.Ed TESL from Universiti Kebangsaan Malaysia (UKM). He has contributed in several researches, publication and innovation competitions both national and internationally. His research interests are in the area of e-Learning, Educational Technology, Adult Learner and Distance Education, Computer Science Education, Multimedia and Gamification.
Email: azlan225@uitm.edu.my