Turkish Journal of Computer and Mathematics Education Vol.12 No. 5 (2021), 1719-1728

Research Article

Cyber Security Behaviorin Online Distance Learning: Utilizing National E-Learning Policy

Siti Daleela Mohd Wahid[1*], Alya Geogiana Buja[2], Noor Afni Deraman[3], Mohd Ali Mohd Isa[4]

[1]Faculty of Business Management, Universiti Teknologi MARA, Malaysia
[3]Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, Malaysia

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: This present study discovers cybersecurity awareness in online distance learning (ODL) during the pandemic crisis. ODL is an excellent way of teaching and learning during this catastrophe. The Government has imposed the National E-learning Policy to support ODL procedures. Unfortunately, the policies have not been carefully planned on security elements. Therefore, by utilizing Information Security Awareness Capability Model and Situation Awareness-Oriented Cyber Security Education Model, we able to: (1) design the security elements for National e-Learning Policy (2) develop a conceptual model of security behavior that benefits ODL procedure. Principally, four factors are demanding attention in the domain of cybersecurity features. On the other hand, there are partially supported hypotheses between the dimensions of cybersecurity and behaviour. Nutshell, we believe our paper is extending the body of knowledge in cybersecurity elements, awareness, and behaviour literature. Future direction, limitation, and conclusion have been thoroughly discussed.

Keywords: Cybersecurity awareness, cybersecurity behavior, National e-learning policy, pandemic, online distance learning.

1. Introduction

The urged by the Ministry of Education (MOE) to switch the teaching and learning from the traditional classroom to advance online class due to the Covid-19 catastrophe is an eye-opener to everybody. At the moment, the schools and higher learning institutions (HLIs) are demanded to use online distance learning (ODL) as the medium of teaching and learning. Online distance learning (ODL) is a method of educating at a distance which utilizes technology combined with traditional education.

ODL offers the concept of anytime and anywhere learning, which encourages lifelong learning and eliminates the problems associated with distance. The flexibility which ODL offers to the students is the main motivating factor in choosing online courses [1]. Besides, ODL helps to advance communication and encourage involvement between the student and the lecturer. ODL also offers faster delivery of assessments, as lecturers can respond faster than the traditional way.

Aware of the significance of ODL in education, MOE has launched the National eLearning Policy (DePAN 1.0 and DePAN 2.0) to be in line with the implementation phases of the National Education Blueprint (Higher Education) 2015–2025 to support the ODL approach. However, both DePAN 1.0 and DePAN 2.0 policies have not cautiously planned the security elements. Past scholars confirmed that it is important to appropriately shield all information in whatever forms to avoid a wider variety of threats and vulnerabilities, such as loss of confidentiality, integrity, and availability [2].

Besides, [3] revealed that it is essential for every individual to know and be aware of cyber risk. Most importantly, they pointed out that hackers tend to seek out the most susceptible users (e.g., those deficient in information and network security awareness). Hackers are proficient at manipulating both software bugs and security gaps unintentionally, which were created by users themselves. The interesting about this paper is we grant the need to investigate (1) the security elements that can be embedded in the National eLearning Policy and (2) influential factors of security behavior in ODL procedures. We structured our paper accordingly which in Section 2, this paper reviews related works on the National e-Learning Policy, cybersecurity elements: awareness and behavior. Meanwhile, Section 3 discusses on methods and materials. Results and discussion have been reviewed in Section 4 and the conclusion is debated in Section 5.

2. Related works

A. Overview of the National E-Learning Policy

In Malaysia, there are two policies introduce by the Government related to e-learning implementation which included National e-Learning Policy (DePAN 1.0) and DePAN 2.0. Further elaborations are as follows:

1. National e-Learning Policy (DePAN 1.0):The first National eLearning Policy, or in the Malay language, Dasar e-Pembelajaran Negara (DePAN) was endorsed in 2011 to offer a direction for the enforcement of e-

Learning in HLIs. Collaborative learning is the key to ensure success in teaching and learning [4]. DePAN 1.0 was made with five essential pillars. Every pillar had its own activities to be executed during the implementation phases, namely, the Early Phase (2011–2012), the Implementation Phase (2013–2014), and the Mature Phase (2015 onwards).

2. National e-Learning Policy (DePAN 2.0): The DePAN 2.0 has not launched yet but has revised new implementation phases to ensure in line with the National Education Blueprint (Higher Education) 2015–2025. DePAN 2.0 has six pillars and aims to certify that Malaysia's quality of education is equivalent to the global standard. The focus of National Education Blueprint (Higher Education) 2015–2025 is on Globalized Online-Learning (GOL). The agenda of GOL is to expand educational accessibility, improve the quality of teaching and learning as well as enable-learning to be tailored to the current needs of the students.

Amongst the efforts done are enhancing the quality of course delivery, reducing the cost of delivery, introducing Malaysia's expert globally, enriching the branding of local HLI, and fostering lifelong learning among Malaysians. GOL is a platform to ensure education is accessible to all communities. Malaysia intends to become the premier hub for education through GOL. Therefore, the National e-Learning Policy (DePAN 1.0) needs to be reviewed appropriately to incorporate with National Education Blueprint (Higher Education) 2015–2025 agenda to improve teaching and learning quality, promoting Malaysian education as well as establishing its prominence in the global education landscape. Unfortunately, shifting DePAN 1.0 to DePAN 2.0 is a never-ending story when ignoring the elements of security. Cybersecurity is needed to protect all shared information from threats. With advanced technology, data can easily be manipulated, hacked and stolen [5].

Proposed Security Elements for National e-Learning Policy: Reviewing the policies, we found that both policies were not carefully planning for the security elements. The idea of security is to protect information from any threats. To protect the information, the guideline in Information Security Management (ISM) is referred. ISM is a policies, process, procedures, organizational structures, and software and hardware functions and needs to be implemented in order to manage the risks.

There are ten domains listed in the handbook of ISM, and all of these domains are very important, and each should be considered when guaranteeing the security of information. As shown in Figure 1, the ODL scenario, it is principally demanding attention in the domain of cybersecurity feature: (CSF1) authentication and accountability, (CSF2) access control, (CSF3) protection of communication, and (CSF4) non-repudiation issues. The enforcement of cybersecurity must be together with the e-learning policy because the e-learning policy comprises of pillars that might be vulnerable and can be compromised by intruders.

a. Authentication and Accountability

Authentication provides a way of identifying a user and is a vital process for ODL since there are numerous platforms used to implement ODL. To ensure all shared information during the ODL session is protected, users are demanded to enter a username and password before being granted access to the system [5].

b. Access Control

As with any other online system, users are given privileges based on their account. These privileges are typically tied to the role assigned to the user. The role will then determine the action that can be carried out by the users, also known as access control or role-based access control, since the role will determine the level of access.

c. Protection of Communication

In the traditional online learning practice, communications usually are carried out in an asynchronous mode via chat module or via discussion. This is due to limitations of available bandwidth in delivering voice or video. So then, the security of communications depends on the security of the database in protecting the data. As technology advances are available, the online classes and discussions can be performed synchronously between teachers and students. Some of the well-known video conferencing software are Webex, Microsoft Teams, Google Meet, and Zoom.

d. Non-repudiation

In an online transaction, it is essential that the user can be held responsible for the action that they had carried out. In cybersecurity, this is known as non-repudiation, which provides proof of the origin of the data and its integrity. Certain activities in ODL require non-repudiation to be implemented, especially for activities that influence grading, such as submitting an assignment or taking a quiz. Hence logging mechanisms that record all users' activities are required.

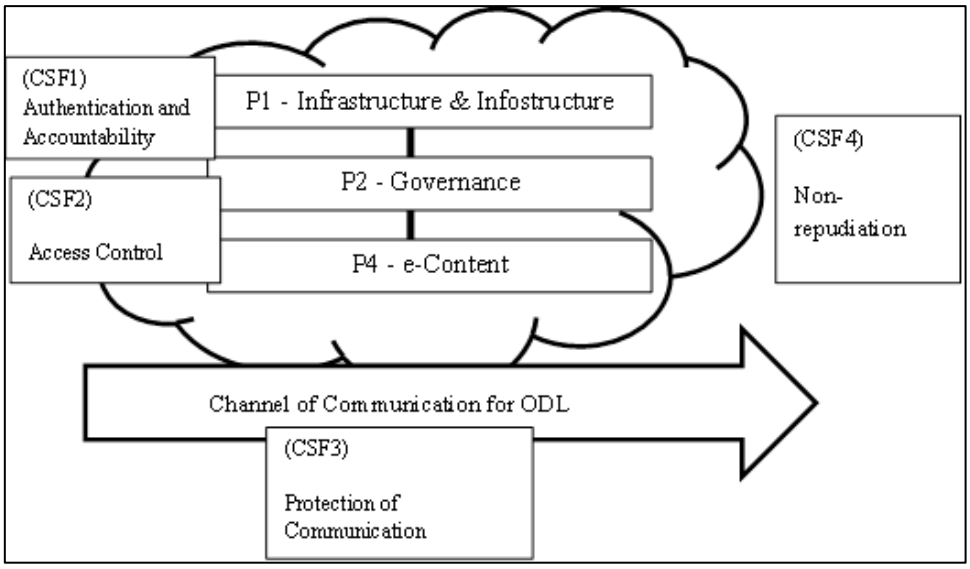

Figure 1: Proposed Security Elements for National e-Learning Policy

B. Factor Influencing Security Behavior

After determining the CSF that potentially embedded in the e-learning policies, we are interested to discover the influential factors lead to security behavior. The reason behind this exploration is to know the level of security behavior among Malaysian. We utilized two prominent models, which is Information Security Awareness Capability Model (ISACM) and Situation Awareness-Oriented Cyber security Education (SAOCE) to identify the most suitable factor associate to security behavior. Theoretically, both theories highlight the importance of security awareness as the precursor to security behavior [6][7].

The design of ISACM comprises three key features which all these features are according to the controls listed within ISO/IEC 27002. The first feature is awareness of the importance in which people's awareness about cybersecurity control will influence the process of successfully avoiding being a scam victim. The second key feature is awareness capability, which refers to how capable a person when dealing with a problem. For example, how a person can understand the type, characteristic, and situation of scam activity. This understanding could influence the rate of successful scam avoiding. Finally, the awareness risk investigated the gap between the amount of awareness importance being more significant than the amount portrayed by a person (awareness capability).

Another advanced model is called SAOCE. This approach was explained by [7] in his research on developing a cybersecurity education curriculum for university students. The approach was based on Situation Knowledge Reference Model (SKRM), which captures the students' awareness on the cybersecurity behavior situations. In the curriculum, several hands-on lab activities representing real-world cyber problems were introduced to bring the conceptual knowledge unit. The advantage of this approach is it has been proven beneficial for the university curriculum, in which the students can have an intensive understanding of cyber security backgrounds. On the other hand, this model helps create cybersecurity awareness among students and also the educators. We believe that applying those prominent models into our framework will create security awareness that leads to cybersecurity behaviour.

1. Security Awareness and Security Behaviour: Initially, [2] defined the term security awareness as "the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks". From the definition, they mentioned that it is essential to every individual to have knowledge and awareness of cyber risk. Most significantly, they postulated that hackers tend to seek out the most susceptible users (e.g., those deficient in information and network security awareness).

On the other hand, [8] noted that attending cyber training programs cannot guarantee individuals will behave more steadily when opposed to a cybercriminal incident. The security training should educate individuals to understand the cybersecurity aspects such as password protection awareness and the ability to secure computers pre, during and post-cyber security training. Notably, cyber education/training's critical role is to emphasize appropriate security practices to improve day-to-day online behavior.

According to [9], the crucial factor in cybersecurity behavior is the individual's cybersecurity awareness. An individual with low awareness behavior is those who are not paying attention or neglecting security alerts. A medium awareness person may be categorized by carelessness explicit in inappropriate technology operation. Lastly, individuals with high awareness comprise knowledge of cyber threats and are capable of taking action in their prevention. Therefore, it is crucial to be aware of any cybersecurity incidents.

Empirically, [10] postulated that awareness plays a significant role in decreasing cyber risk behavior. In other words, early exposure to cyber training programs pushed individuals to use complex passwords. They recommended that providing security awareness training courses can comprehensively impact attitudes to cybersecurity management. In other development, [11] emphasized that it is vital to offer cyber training programs at school or HLIs level. Literally, we need to declare that the literature tends to call for more research to address the relationship between individual awareness and self-reported behavior in cybersecurity processes. The proposed conceptual framework is presented in Figure 2.

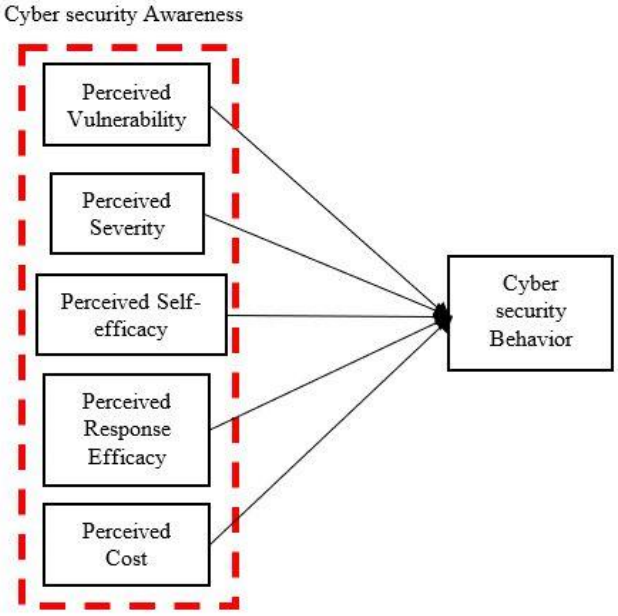

Figure 2: Development of Cybersecurity Behaviour

3. Method and materials

A. Population and Sample

This study population consisted of educators and students in Malaysia. The data collection process encompassed an online survey questionnaire that was implemented via Google form. Although using the self-reported, we conducted Harman's One Factor Solution analysis, which allows controlling for common method variance (CMV) [12], which was essential for this study. Data collection took place on 15 June 2020 and lasted for eight weeks. For this current study, we employed the non-probability sampling category, namely the convenience sampling technique. The convenience sampling technique refers to sampling plans where the sample of the population who are conveniently available to respond. The advantage of this sampling technique is quick and convenient [13]. As for sample size, few guidelines have been suggested by past scholars. Once decided, we considered 300 samples.

B. Measurement and Scaling

The online survey questionnaire was designed into two (2) sections. The questions in section A covered the factors influencing cybersecurity awareness and behavior. All items were borrowed and improvised from [14]. Later, it was altered to suit the studied context. The entire instruments used a 7-Likert scale ranging from 1 (Completely Disagree) to 7 (Completely Agree) to measure the items. The questions in section B covered the respondent's profiling characteristics, such as gender, age group, and race, were all collected in this study.

C. Analytical Strategy

In this paper, we used two statistical packages for analyzing the data. First, Statistical Package for the Social Sciences (SPSS) software was employed for descriptive analysis. Second, Analysis Moment of Structures (AMOS) software was used for Structural Equation Modelling (SEM) analysis. According to [15], Structural Equation Modeling (SEM) "is the best multivariate procedure for testing both the construct validity and theoretical relationships." SEM is more compelling approach as compared to other analysis of co-variance. It added that by using SEM, the strength of associations between constructs could be identified more precisely because it considers measurement errors.

Besides, SEM strategy also allows the comparison of alternative and relative models, making it more robust. 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 is 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. 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 analyzing multi-dimensional constructs which consist of multiple underlying concepts [16]. Investigating a theory using the software is fast, efficient, and user-friendly [17]. This software is popular because of its attributes- explanatory ability and statistical efficiency for model testing. A single comprehensive procedure can reduce measurement errors and provide a better understanding of the studied phenomenon.

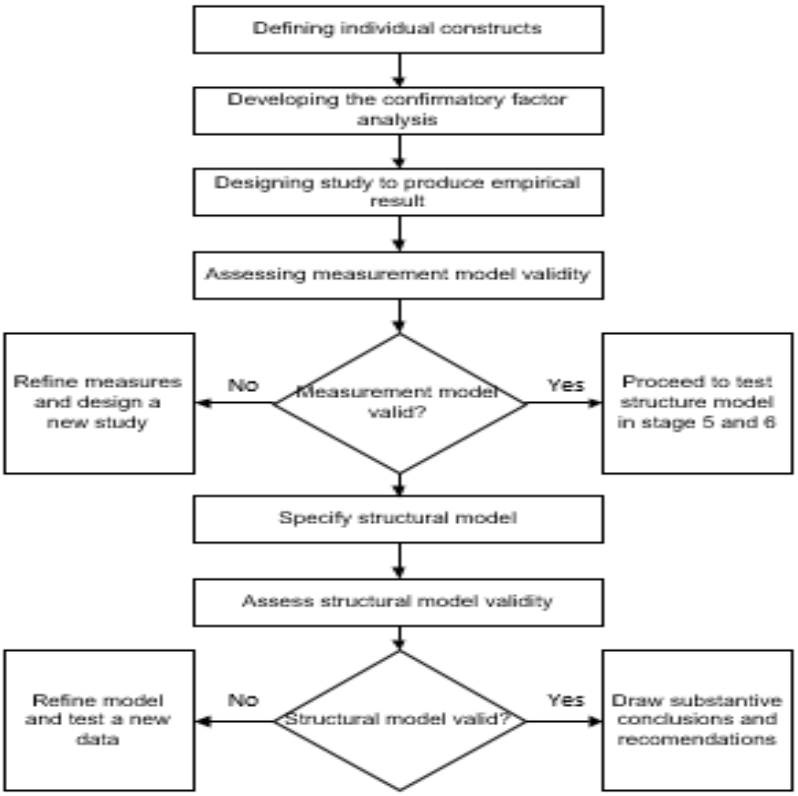

Figure 3: Stages for Structural Equation Modeling

4. Results and Discussion

A. Demographic Profile

Table 1 shows the demographic profile for the students and educators who responded to the questionnaire. The 300 respondents who took part in this survey were 56.3% (N=169) males and 43.7% (N=131) females. Most them were 18-29 years old (39.3%, N=118), followed by age group of 30-39 years old (32.0%, N=96), 40-49 years (21.0%, N=63), and above 50 years old (7.7%, N=23). In terms of race, 75.7% (N=227) were Malay, 12.3% (N=37) were Chinese, 6.0% (N=18) were Indian and 6.0% (N=18) were others.

Table 1: Result of the Demographic Profile

Characteristic		Frequency	Percentage
Gender	Male	169	56.3
	Female	131	43.7
Age	18-29 years old	118	39.3
	30-39 years old	96	32.0
	40-49 years old	63	21.0
	Above 50 years old	23	7.7
Race	Malay	227	75.7
	Chinese	37	12.3
	Indian	18	6.0
	Others	18	6.0

B. Assessment on SEM Approach

In this section, we assess four critical elements of SEM. Firstly the confirmatory factor analysis (CFA) and later, measurement model. Third, we will be testing the structural model to confirm hypotheses development. Lastly, we executed CMV procedures through Harman's One Factor Solution analysis.

1. Testing the Confirmatory Factor Analysis (CFA): CFA is a procedure to validate all latent variables in the model. The purpose of conducting CFA is to test the model fit, standard factor loadings, and 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 [18]. In CFA, the theory is proposed first, then tested to see how the constructs systematically represent latent variables. In this paper, ISACM and SAOCE are evaluated first, thereafter, we listed the relevant factors to be studied. In CFA, all constructs are assessed simultaneously. Using this approach, all constructs are pooled and linked using the double-headed arrows to evaluate the correlation among the constructs. The CFA model for six (6) latent variables ranges from 0.723 to 0.932. The model also shows that the correlation coefficients among the constructs range between 0.024 and 0.706, which is less than 0.900; therefore, suggesting no multicollinearity among the variables.

2. Testing the Measurement Model: The first step of SEM is to test the measurement model. The result obtained from the Pooled-CFA process were assessed to form a measurement model. The fit indices values are Relative Chi-Square=2.495, RMSEA=0.060, CFI=0.954, TLI=0.946 and PGFI=0.703. As these fit indices meet the requirement as recommended by [15], who suggested that if three to four of the Goodness-of-Fit (GOF) indices meet the requirement, then the model is acceptable. Hence, in this study, the measurement model is declared to be a good fit. The summary of the model fit for the measurement model are shown in Table 2.

In the measurement model, we also tested convergent validity, discriminant validity, and construct reliability. Convergent validity refers to a set of variables or items that are assumed to measure a construct and share a high proportion of common variance. It is tested by using factor loadings and average variance extracted (AVE). Both factor loadings and AVE should measure a minimum of 0.500, which indicates high convergent validity. Composite reliability (CR) refers to the degree to which an instrument is measured according to the constructs' dimensions. The acceptable cut-off point of CR is in between 0.600 to 0.700. The overall result is presented in Table 3.

Discriminant validity refers to "the extent to which a construct is truly distinct from other constructs" [15]. It also means that factors or items only measure one latent construct. The cut-off point 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, findings showed that the r2 of all variables' values are less than AVEs'. Consequently, it indicated that each construct is distinct.

3. Testing the Structural Model: The second step in SEM is to test the structural model by examining the hypothesized relationships among latent variables. The structural model denotes one endogenous relationship linking the hypothesized model's variables. In this study, the structural model's focus is to examine and test the interrelationship between exogenous and endogenous variables. This present study adopted the Total Disaggregation Structural Model, involving only latent variables. A total of 5 hypotheses were analyzed.

As the aim of testing the structural model is to examine the interrelationship between exogenous (PV, PS, PSE, PRE, and PC) and endogenous (CB) variables. The results are presented in Table 5, showing mixed results. The H1, H3 and H5 showed a significant relationship between them, β=0.511, p=0.000; β=0.238, p=0.000; β=0.306, p=0.000 respectively. Meanwhile, H2 and H4 stated an insignificant relationship, β=-0.058 p=0.229; β=0.027, p=0.459 accordingly.

4. Testing the CMV Procedure: To conduct the Harman's One Factor Solution test, CFA was performed, which is a more refined analysis of the test [19]. Two models were developed: a Harman's One Factor and a measurement model. For Harman's One Factor, all items were loaded on one general factor. Then, the model fit of the Harman's One Factor model was compared with the model fit of the proposed measurement model. If Harman's One Factor model had a poor fit compared to the proposed model, CMV 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 confirms that CMV is not a problem in this study.

We reviewed the deficiency of security elements in the National e-Learning Policy. Although our Government improvised the DePAN 1.0 to DePAN 2.0, it will never be an ending story if we ignored security elements. Past scholars confirmed lack of cybersecurity awareness would increase the cyber risk among people, especially students. With the world pandemic outbreak, it required all teaching and learning conducted on an online basis. Without proper security awareness, there is no point in executing ODL.

With that in mind, we investigated the influential factors that lead to cybersecurity behavior among students and educators. We identify five dimensions, namely PV, PS, PSE, PRE, and PC of cybersecurity awareness, which theoretically supported the linkage to cyber behavior. Our findings show that the respondents' PV, PSE, and PC had a significant connection to cybersecurity behavior. The number of phishing scam victims were increasing year by year. It is suggested that all students, educators, or even senior adults attend the cyber training program to help them act securely when confronted with a cybersecurity incident. Literature confirmed that

attending cyber training programs, it able to reduce the number of scam victims. Since this connection was found, it highlights the significant role of educational cybersecurity programs to enlarge cyber-attack awareness.

Even though practicing cyber awareness is costly and time-consuming, the respondents agree that investing in such cyber training helps them become cyber victims. Past scholars postulated that when the cyber tools available are simple and familiar to the users, they are more aware and take careful steps to prevent attacks. On the other hand, if it required specialized or complicated knowledge in handling the cyber tools, the interplay was more complex [20].

We found there is no connection between PS and PRE on cybersecurity behavior. We found that our result is in line with the research by [21][22]. In their studies, both stated most employees felt safe and did not want to understand the cyber protection tool available by transferring the role to the organization. Alternatively, [23] and [24] proposed that cybersecurity training should be made mandatory for all employees. It also suggested that the course should be problem-centered, utilizing case studies tailored to levels of awareness. Then, it probably would increase the PS and PRE.

Table 2: Result of Measurement Model

	AFI		**IFI**		**PFI**
Fit Indices	Relative Chi Square [<5]	RMSEA [<=0.080]	CFI [>=0.900]	TLI [>=0.900]	PGFI [>=0.500]
Measurement Model	2.495	0.060	0.954	0.946	0.703

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: Result of Convergent Validity and Composite Reliability

Constructs	**Items**	**Factor loadings(>0.500)**	**AVE(>0.500)**	**CR**
Perceived Vulnerability (PV)	PV1	0.844	0.642	0.843
	PV2	0.831		
	PV3	0.723		
Perceived Severity(PS)	PS1	0.718	0.600	0.818
	PS2	0.818		
	PS3	0.784		
Perceived Self-Efficacy (PSE)	PSE1	0.932	0.794	0.939
	PSE2	0.928		
	PSE3	0.846		
	PSE4	0.855		
Perceived Response Efficacy (PRE)	PRE1	0.798	0.696	0.902
	PRE2	0.821		
	PRE3	0.882		
	PRE4	0.835		
Perceived Costs (PC)	PC1	0.854	0.663	0.887
	PC2	0.798		
	PC3	0.822		
	PC4	0.781		
Cybersecurity Behavior (CB)	CB1	0.877	0.746	0.936
	CB2	0.888		
	CB3	0.848		
	CB4	0.890		
	CB5	0.814		

Table4: Result of Convergent Validity and Composite Reliability

Tested path	AVE_1	AVE_2	RESULT
PV ⟷ PS	0.642	0.600	Valid
PV ⟷ PSE	0.642	0.794	Valid
PV ⟷ PRE	0.642	0.696	Valid
PV ⟷ PC	0.642	0.663	Valid
PS ⟷ PSE	0.600	0.794	Valid
PS ⟷ PRE	0.600	0.696	Valid
PS ⟷ PC	0.600	0.663	Valid
PS ⟷ CB	0.600	0.746	Valid
PSE ⟷ PRE	0. 794	0.696	Valid
PSE ⟷ PC	0.794	0.663	Valid
PSE ⟷ CB	0.794	0.746	Valid
PRE ⟷ PC	0.696	0.663	Valid
PRE ⟷ CB	0.696	0.746	Valid
PC ⟷ CB	0.663	0.746	Valid
PV ⟷ CB	0.642	0.746	Valid

Notes: PV- Perceived vulnerability, PS-perceived severity, PSE- perceived self-efficacy, PRE- perceived response efficacy, PC-perceived cost, CB-cyber security behavior.

Table5: Result of Hypothesis Testing

H	Causal Path	β	E	S.E.	C.R.	p
H_1	PV→CB	0.511	0.468	0.045	10.332	***
H_2	PS→CB	-0.058	-0.051	0.043	-1.202	0.229
H_3	PSE→CB	0.238	0.172	0.035	4.915	***
H_4	PRE→CB	0.027	0.029	0.039	0.741	0.459
H_5	PC→CB	0.306	0.360	0.053	6.786	***

Notes: H- Hypothesis, E- Estimate, PV- Perceived vulnerability, PS- perceived severity, PSE- perceived self-efficacy, PRE- perceived response efficacy, PC- perceived cost, CB-cyber security behavior.

Table6: Result of CMV

	AFI		IFI		PFI
Fit Indices	Relative Chi Square [<5]	RMSEA [<=0.080]	CFI [>=0.900]	TLI [>=0.900]	PGFI [>=0.500]
Measurement Model	2.495	0.060	0.954	0.946	0.703
Harman's One Factor Solution Model	17.813	0.201	0.450	0.395	0.389

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 present study was driven by the discrepancy in the National e-Learning Policy. We identify four CSF, namely authentication and accountability, access control protection of communication, and non-repudiation embedded in the national policy. Besides, we explored five dimensions of cybersecurity awareness influencing cybersecurity behavior. Unfortunately, the literature for these variables showed few theoretical and empirical studies on the relationship between factors stimulating cyber behavior conditions. Empirical evidence on cyber security behavior was limited, thus enabling us to study the relationship between these variables among students and educators in the Malaysia context.

Despite the contributions yielded from this study, the findings should be interpreted within the limitation of the methodology employed. Firstly, this study applies the method of quantitative research design and the data collected via questionnaire survey. Although quantitative research methods can be used to ascertain the degree to which individuals undertake behaviors, it limits the ability to analyze the thoughts and feelings of research participants as well as the meaning that respondents ascribe to their experiences. Future work should use a mixed-method approach to compounding quantitative and qualitative data to better explain cyber security behavior. A combination of quantitative and qualitative analyses probably will reinforce findings related to cyber behavior. Secondly, this present study is drawn on cross-sectional data due to time and financial resource constraints. Thus, although the findings are presented as a cause-effect phenomenon, the data is not explicitly measured over time. Yet, data has been widely applied by most studies on science and technology research.

Acknowledgements

Sincere appreciation goes to Universiti Teknologi MARA Cawangan Melaka for the support given to this research endeavor, TEJA: Internal Grant (GDT2020-17).

References

1. Najwa Hayaati, M.A., Ip-Shing, F. “E-learning and information security management”, International Journal of Digital Society, 1:148-156, (2010).
2. Villanueva, J. A., Lacatan, L. L., Vinluan, A. A. “Information technology security infrastructure malware detector system”, International Journal of Advanced Trends in Computer Science and Engineering, 9(2): 1583–1587, (2020).
3. Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J. “The impact of information richness on information security awareness training effectiveness”, Computer Education, 52: 92–100, (2009).
4. “Buletin Pembangunan Akademik UKM”. Malaysia: UKM Press, (2011).
5. Salimovna, F., Yuldasheva, N., Ugli, I. “Security issues in E-Learning system”, 1: 1-4, Available online: 10.1109/ICISCT47635.2019.9011971, (2019).
6. Poepjes, R., Lane. M. “An information security awareness capability model”. Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3-5 December 2012.
7. Dai, J. “Situation awareness-oriented cybersecurity education”, IEEE Frontiers in Education Conference, 1: 1-8, (2018).
8. Cain, A., Edwards, M.E., Still, J.D. “An exploratory study of cyber hygiene behaviors and knowledge”, Journal of Information Security Application, 42: 36-45, (2018).
9. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., Basim, H.N. “Cyber security awareness, knowledge and behavior: A comparative study”, Journal of Computer Information Systems, 60:1-16, (2020).
10. Eminağaoğlu, M., Uçar, E., Eren, Ş. “The positive outcomes of information security awareness training in companies–a case study”, Information Security Technical Report, 14: 223–229, (2009).
11. Bong-Hyun, K., Ki-Chan K. “Development of cyber information security education and training system”, Multimedia Tools Application, 76: 6051-664, (2017).
12. Podsakoff, P.M., Mackenzie, S.B., Lee, J-Y., Podsakoff, N.P. “Common method biases in behavioral research: A critical review of the literature and recommended remedies”, Journal of Applied Psychology, 88: 879-903, (2003).
13. Sekaran, U., Bougie, R. “Research Methods for Business: A Skill Building Approach”, 7th Edition. Singapore: John Wiley & Sons (Asia) Pte. Ltd., (2016).
14. Simonet, J., Teufel, S. “The influence of organizational, social and personal factors on cybersecurity awareness and behavior of home computer users”, In G. Dhillon et al. (Eds.): SEC 2019, IFIP AICT, 562: 194–208, (2019).
15. Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. “Multivariate Data Analysis”, 8th Edition. Andover: Cengage Learning, EMEA, (2018).

16. Byrne, B.M. “Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming, Multivariate Applications Series”. 3rd Edition. USA: Routledge, (2016).
17. Zainudin, A. “SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling”, Bangi, Malaysia: MPWS Rich Publication, (2015).
18. Kline, R.B. “Principles and Practice of Structural Equation Modeling”, 4th Edition. New York: The Guilford Press, (2016).
19. Zaefarian, G., Henneberg, S. C., Naudé, P. “Assessing the strategic fit between business strategies and business relationships in knowledge intensive business services”, Industrial Marketing Management, 42: 260-272, (2013).
20. Skripak, I. A., Aynazarova, S. N., Vladimirovna, E., Tkachenko, A. E., & Erina, L. S. “Digital virtualization technologies in distance learning”, Advanced Trends in Computer Science and Engineering, 9(2): 1808–1813, (2020).
21. Hadlington, L., Parsons, K. “Can cyberloafing and Internet addiction affect organizational information security?”, Cyberpsychology Behavior Social Networking, 20: 567-571, (2017).
22. Tischer, M., Durumeric, Z., Foster, S, Duan, S., Mori, A., Bursztein, E., Bailey, M. “Users really do plug in USB drives they find”, IEEE Symposium on Security and Privacy, 1: 306–19, (2016).
23. Abawajy, J., Kim, T.H. “Performance analysis of cyber security awareness delivery methods. Security technology, disaster recovery and business continuity”, Communication in Computer and Information Science, 122: 142–48, (2010).
24. Pawlowski, S.D., Jung, Y. “Social representations of cybersecurity by university students and implications for instructional design”, Journal of Information System Education, 26:281–94, (2015).