European Journal of Computer Science and Information Technology
Vol.10, No.1, pp.1-9, 2022
Print ISSN: 2054-0957 (Print),
Online ISSN: 2054-0965 (Online)

EFFECTS OF PEOPLE'S MENTAL MODELS OF CYBERSECURITY ON THEIR SECURITY BEHAVIOUR

Nwokeji, C. E. and Agubosim, Chuka C.
[1]Department of ICT Chukwuemeka Odumegwu Ojukwu University, Anambra- Nigeria
[2]Department of Computer Science Chukwuemeka Odumegwu Ojukwu University, Anambra-Nigeria

ABSTRACT: *This research investigates the effects of people's mental modal of cybersecurity on their security behaviour. Data were collected using survey design and the questions were measured on a Likert five point-scale. The questionnaires were distributed to mainly IT staff, management staff and other staff that uses computers in the discharge of their duties. The data were analysed using percentages, frequencies and statistical methods of regression and ANOVA while Cronbach Alpha reliability coefficient technique was adopted to test the validity of the questions used to collect primary data. The result reveals that people's prior knowledge of cybersecurity issues has no effect on people's mental models for improved cybersecurity behaviour, but lack of trained staff (cyber talents), lack of supportive infrastructures, time constraints, exclusion of cybersecurity in non-computing courses, poor knowledge of fundamental computing areas, lack of mentors with hands-on experience, lack of cyber training or challenge programme, and inadequate books on cyber security were admitted by the participants as some of the major factors that inhibit their knowledge and engagement in cybersecurity education. These barriers if not checked could limit the level of cybersecurity awareness among undergraduate students.*

KEYWORDS: cybersecurity, cyberspace, mental models, security behaviour

INTRODUCTION

The twenty-first century has witnessed tremendous advancement in the operation of interconnected complex systems. This has turned the world into a global village and businesses leveraging on cyber technology for competitiveness and improvement in the lives of humans. This tremendous growth in cyber technology also comes with great concerns to the safety and security of all users as more and more business and private data are being held or transmitted over the cyberspace. To protect organisations and individuals from ravaging cyber-crimes and information theft, a lot of cybersecurity technologies like VPN, IPsec, Firewalls, https, anti-malware, anti-virus among others have been developed to protect users from various types of cyber-attack. However, these advancements in the development of cybersecurity technologies according to Houser (2018) has failed to provide adequate security to the cyber-world due to what is termed human factor. Commenting further, Houser (2018); Hadlington (2018); Blythe & Camp (2012) argued that since the weakest link in the chain of cybersecurity is the human element, understanding of human-computer interaction (HCI) is essential in developing cybersecurity technical solutions.

Volkamer & Renaud, (2013) argue that these cyber technologies prove inadequate as soon as the end-users get involved in using them. Stating that since users' decisions and actions are

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

subject to their mental model, it will be desirable that developers and designers understand users' mental models when developing these cybersecurity technologies. This notion was supported by Pfleeger & Caputo (2012) who urged cybersecurity developers to leverage people's peculiarities and perceptions to provide effective and efficient human-centred security. Computer hardware/software products are mostly developed based on the designer's mental model, not knowing that what designers thought to be easy to understand may not be true to end users in most cases (Xie, Zhou, & Wang, 2017; Albalawi, Ghazinour, & Melton, 2017). However, they assert that certain end-users with either incomplete or wrong mental models can still make sound decisions while using computer products in most cases. But dealing with end-users' mental models can be a challenging and daunting task as also opined by (Albalawi et al., 2017; Blythe & Camp, 2012). This is because different user groups may exhibit different mental models in a similar situation, and a particular user may exhibit different mental models in different situations. No wonder Wilson & Rutherford (1989) were of the view that user mental models as a concept look somehow incoherent and confusing.

However, if cyber attackers are exploiting human vulnerabilities to bypass various cybersecurity technologies and execute their attacks as opined by (Houser, 2018), human vulnerabilities must also be explored to complement the cybersecurity technologies in defence of cyberspace. And if mental models are truly inseparable from our personalities and sense of who we are as opined by Edward-Leis (2012) who also see mental models as a cognitive structure which are based on past experiences, prior knowledge, new understandings, and existing ideas which are used to explain and interpret events around us; then, can understanding people's mental models of cybersecurity improve security behaviour?

A number of researches has been done on the area of cybersecurity behaviour and people's mental models, while some of the opinion that there is a relationship between people's mental models and cybersecurity behaviours (Albalawi et al., 2017; Berg, 2019; Maier, Padmos, Bargh, & Wolfgang, 2017; Wash & Rader, 2011). Others were not convinced of any cogent relationship between the two (Brase, Vasserman, & Hsu, 2017). This work, therefore, wants to go further to investigate how certain conditions modifies people's mental models and how each affects their security behaviour. To the best knowledge of the researcher, no work has been done on this area and it offers a promising new area of exploration in winning the cyberwar against cybercriminals.

This study intends to investigate the effects of people's mental models of cybersecurity on their security behaviour. Specifically, the study intends to:

- Analyse if people's prior knowledge of cybersecurity issues effects security behaviour.
- Determine the extent to which people's perception of system interface design affect security behaviour.
- Determine if people's procedural knowledge of using systems affect security behaviour.
- Find out whether people's general awareness of privacy threats affect security behaviour.
- Access the extent to which people's cultural peculiarities influence security behaviour.
- To develop an econometric model of people's mental models and security behaviour.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Research Question:

- Does people's prior knowledge of cybersecurity issues improve security behaviour?
- To what extent does people's perception of system interface design affect security behaviour?
- Does people's procedural knowledge of using systems affect security behaviour?
- Does people's general awareness of privacy threats affect security behaviour?
- To what extent does people's cultural peculiarities influence security behaviour?

Research Hypothesis:

The null hypotheses of the study are stated below:

1. Prior knowledge of cybersecurity issues has no effect on peoples' mental models for improved cybersecurity behaviour.
2. Perception of system interface design has no effect on peoples' mental models for improved cybersecurity behaviour.
3. Procedural knowledge of using systems has no effect on peoples' mental models for improved cybersecurity behaviour.
4. General awareness of privacy threats has no effect on peoples' mental models for improved cybersecurity behaviour.
5. Cultural peculiarities have no effect on peoples' mental models for improved cybersecurity behaviour.

METHODOLOGY

Data was collected for this study through questionnaires, structured and semi-structured interviews, and through site observations. The data was collected in two phases, phase one collects data for investigating the people's mental models of cybersecurity. While the phase two of the data collection depended on the outcome of phase one and investigates the complex issues of how the understanding people's mental models of cybersecurity can improve their security behaviour.

In phase one, the questionnaires were structured question and close-ended, based on ISO27002:2005 code of practice. ISO27002:2005 code of practice was used because of its wider adoptability and its simplicity of language. The questions were measured on a Likert five point-scale whereby 1= Strongly Disagreed, 2 = Disagreed, 3 = Undecided, 4 = Agreed, and 5 = Strongly Agreed. The questionnaires were distributed to mainly IT staff, management staff and other staff that uses computers in the discharge of their duties. Phase two questionnaire was designed to respond to the outcome of phase one result followed the structure and measurement tools adopted in phase one.

Cronbach Alpha reliability coefficient technique was adopted to test the validity of the questions used to collect primary data. The collected data for this work were analysed using percentages, frequencies and statistical methods of regression and ANOVA.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

RESULTS

A. Reliability Test

The internal consistency reliability for the 20-item is judged based on calculating Cronbach's alpha. For this test, the Cronbach's alpha 0.845. The obtained alpha value proves the adequate internal consistency for the 20-items.

Table 1: Reliability Statistics

Cronbach's Alpha	N of Items
.845	20

B. Respondents' Demographic Information

Table 2: Gender of the Respondents

Subjects	Freq.	Percent	Valid Percent	Cumulative Percent
Male	140	70.0	70.0	70.0
Female	60	30.0	30.0	100.0
Total	200	100.0	100.0	

Table 2 depicts the distribution of respondents by gender. It can be inferred from the table that 70% of the respondents were males while 30% were females. This implies that majority of the respondents were females.

Table 3: Age Distribution of the Respondents

Age Range	Frequency	Percent 1
18-25yrs	133	66.5
26-34yrs	39	19.5
35 years and above	28	14.0
Total	200	100.0

Table 3 above shows the distribution of respondents by age. It indicates that 66.5% of the respondents were within the age of 18-25 years, 19.5% were 26-34 years old, while 14.0% of the respondents were 35 years and above. This implies that the majority of the respondents were within the age of 18-25 years old.

Regression Analysis Interpretation

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.661a	.415	.238	. 557

A. Predictors: Level of awareness of Cyber Security issues

Table 4 provides the R and R2 values, adjusted R squared, and the standard error. The Rvalue is the multiple correlation coefficient, represents the simple correlation and is 0.661 (the "R" Column), which indicates a moderate degree of correlation. The R2 value (the "R Square" column) indicates how much of the total variation in the dependent variable can be explained by the independent variables. The model fits the data gotten from the sampled questionnaire Nigeria because of the value of 0.415 thus optimistically estimate how well the

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

model fits the population. This is also justified by the adjusted R squared with value 0.238 which has attempted to correct R squared to more closely reflect the goodness of fit of the model in the population. In this case, 23.8% of the dependent variable can be explained by the independent variables.

Table 5: ANOVA Results

Model	Sum of Squares	DF	Mean Square	F	Sig.
1 Regression	45.538	20	1.776	4.111	.000a
Residual	67.547	179	.432		
Total	113.085	199			

a. Independent variables: People's mental awareness level of Cyber security
b. Dependent Variable: Interest in Cyber security issues

Table 5 summarizes the results of an analysis of variance (ANOVA). The sum of squares, degree of freedom (DF), variation, regression, and residual. The output for the regression displayed information about the variation accounted for by the model. And the output for total is the sum of the information for regression and residual. The model accounted for most of the variation in the dependent variable because of the value (45.538) of the regression sum of squares in comparison to the residual sum of squares value of 67.547. And the model did justice to this because of the residual sum of squares; 67.547. From table5, the Significance value is 0.000 (i.e., p = .000), which is below 0.05 and, therefore, there is a statistical significance between the variables.

Table 6: Coefficient

Model	Unstandardized Coefficients		Standard Coefficients	T	Sig.	95.0% Confidence Interval for B	
	B	Std. Error	Beta			Lower Bound	Upper Bound
1 (Constant)	.424	.130		3.253	.001	.167	.681
Awareness level	.056	.025	.078	2.217	.028	.006	.106
Interest in Cybersecurity Education	.065	.027	.110	2.407	.017	.012	.118

a. Independent variables: People's mental awareness level of Cyber security
b. Dependent Variable: Interest in Cyber security issues

The T statistics in table 6 helped us to determine the relative importance of each variable in the model. The relative importance is determined with the T values well below -2 or above +2. The People's mental awareness and their attitude'/interests T values are above +2 with respective values of 2.217 and 2.407. The foregoing statement showed that all the independent variables are of relative importance to determine the awareness level of cyber security among the people and their interest in cybersecurity issues. The independent variables do a good job explaining the variation in the dependent variable because of the small significance value of the F statistic 0.000 which is smaller than 0.05, which means that a relationship does exist between the variables.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Table 7: Testing of Hypotheses

Hypotheses Variable Name	P-Value	Statistically Significant	Null Hypothesis Accept/Reject
H1 Level of awareness and perceptions of Cybersecurity	.014	Statistically significant	Rejected
H2 Cybersecurity awareness and interest in cybersecurity issues	.036	Statistically significant	Rejected

The second column shows the predictor variables. The coefficient table contains the values for the regression equation for predicting the dependent variable from the independent variable. These are also the values for 95% confidence intervals for the coefficients. From table 7, the null hypothesis i.e, H1, and H2 are rejected. It indicates that the level of awareness of Cyber Security among the people has significant effect on their perceptions of cyber-Security and their interests in Cyber security issues.

The Barriers to Cyber Security Education among Undergraduates

The barriers that impede cyber security awareness or education among the undergraduate students were examined using Principal Axis Factoring (PAF) with Promax rotation. The initial inspection of the Rmatrix indicated a substantial number of the coefficients were above .30. The KaiserMayer-Olkin (KMO) index was 0.79, exceeding the recommended value of 0.6 [26], and Bartlett's Test of Sphericity [27]. reached statistical significance ($\chi 2=565.89$, $p<.001$), indicating that the data were suitable for factor analysis. The results of the initial analysis revealed three factors with Eigenvalues over 1, explaining 34.370%, 20.848%, and 8.375% of the variance, respectively (Table 8).The first identified component has Eigenvalue more than 1.0, and the variables have factor loading of 0.5 or more, can be chosen as a cut-off for acceptable loadings because they were noteworthy to determine the minimum loading necessary to comprise an item [28]. Following the best practices of item retention outlined at the outset, twelve items were retained for the final analysis with three latent factors. Five items (Lack of trained staff (cyber talents), lack of appropriate infrastructure, time constraints, lack of interest, exclusion of cybersecurity in noncomputing courses) loaded on factor 1, another five items (Poor knowledge of fundamental computing areas like computer architecture and Operating system internals), lack of mentors with hands-on experience, lack of cyber training or challenge program, Inadequate books on cybersecurity, ignorance) loaded on factor 2 and the other two items (Cultural issues, Network issues) loaded on factor 3 (Table 9).

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

Table 8: Total Variance Explained

Factor	Initial Eigen values			
Total	% of Variance	Cumulative %	Total	
1	4.124	34.370	34.370	3.692
2	2.502	20.848	55.218	2.084
3	1.005	8.375	63.593	.529
4	.883	7.360	70.953	
5	.705	5.873	76.825	
6	.586	4.884	81.709	
7	.536	4.469	86.179	
8	.427	3.557	89.735	
9	.381	3.177	92.912	
10	.339	2.828	95.740	
11	.311	2.593	98.333	
12	.200	1.667	100.000	

Table 9: Standardized Factor Loadings from the Exploratory Factor Analysis on the barriers that inhibit cybersecurity education

	Factor		
Items	1	2	3
Lack of trained staff (cyber talents)	.907		
Lack of appropriate infrastructure	.798		
Time Constraints	.646		
Lack of interest	.597		
Exclusion of Cybersecurity in noncomputing courses	.432		
Poor knowledge of fundamental computing areas		.844	
Lack of mentors with hands-on experience		.792	
Lack of cyber training or challenge programme		.768	
Inadequate books on Cyber security		.471	
Ignorance		.420	
Cultural issues		.711	
Network issues		.653	

DISCUSSION

The result shows that the participants had only basic knowledge of Cybersecurity. Many of the participants were aware of cyber threats, but had low knowledge about how to protect themselves from the various cyber threats and attacks. Hence, we regard their knowledge of cybersecurity as being basic or low. The results showed that people's prior knowledge of cybersecurity issues has no effect on people's mental models for improved cybersecurity behaviour. Majority of the participants believed that cyber security knowledge is important considering the increasing use of internet and rising cases of cybercrimes. A significant statistical relationship was also observed between the level of people's awareness and their interests in cybersecurity issues. Many participants who were aware of cyber security threats indicated their interests and willingness to engage more in cybersecurity education programme.

@ECRTD-UK- https://www.eajournals.org/
https://doi.org/10.37745/ejcsit.2013

(Kam and Katerattanakul) posited that high student engagement increases student interests in cybersecurity. Hence, more engagement of students in cybersecurity issues would enhance their cyber skills. On the barriers that impede cybersecurity awareness or education among people, our findings revealed that; lack of trained staff (cyber talents), lack of supportive infrastructures, time constraints, exclusion of cybersecurity in non-computing courses, poor knowledge of fundamental computing areas, lack of mentors with hands-on experience, lack of cyber training or challenge programme, and inadequate books on cyber security were admitted by the participants as some of the major factors that inhibit their knowledge and engagement in cybersecurity education. These barriers if not checked could limit the level of cybersecurity awareness among undergraduate students.

CONCLUSION

Cybersecurity awareness or education is now a necessity than ever because of the high penetration of the internet which has become a haven for cyber criminals. Thus, organizations should rise to the occasion and put measures in place to protect themselves from cyber threats and internet fraudsters. Also, cybersecurity should be included as a core course for all undergraduate programmes, especially science related courses in higher education. This would assist students, teachers and indeed institutions and organizations to know more about cyber threats and how best to protect themselves from cyber criminals. Finally, there is also the need for promotion of cultural or moral values to dissuade young people from engaging in cybercrimes.

References:

Albalawi, T., Ghazinour, K., & Melton, A. (2017). Security Mental Model : Cognitive map approach. In *International Conference on Computational Science and Computational Intelligence*.

Berg, J. Van Den. (2019). Grasping Cybersecurity : A set of Essential Mental Models. In *European Conference on Cyber Warfare and Security* (p. 2019).

Blythe, J., & Camp, L. J. (2012). Implementing Mental Models. *2012 IEEE Symposium on Security and Privacy Workshops*. https://doi.org/10.1109/SPW.2012.31

Brase, G. L., Vasserman, E. Y., & Hsu, W. (2017). Do Different Mental Models Influence Cybersecurity Behavior ? Evaluations via Statistical Reasoning Performance. *Frontiers in Psychology*, *8*(November), 1–9. https://doi.org/10.3389/fpsyg.2017.01929

Chandarman, R & Van B. (2017). "Students Cybersecurity Awareness at a private tertiary educational institution. *The African J. of Info. and Comm. (AJIC)*, Vol. 20, pp 133-155

Edward-Leis, C. (2012). Challenging learning journeys in the classroom : Using mental model theory to inform how pupils think when they are generating solutions. In *PATT 26 Conference; Technology Education in the 21st Century* (pp. 153–162). Stockholm: Linköping University Electronic Press.

Garba, A., Siraj, M., Othman, S., & Musa, M. (2020). "A study of Cybersecurity Awareness among students in Yobe State University, Nigeria: A Quantitative Approach". *International Journal of Emerging Technologies*, vol 11 No 5 pp 41-49

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online

Behaviours : An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology*, *12*(1), 269–281. https://doi.org/10.5281/zenodo.1467909

Houser, A. M. (2018). *Mental Models for Cybersecurity : A Formal Methods Approach*. State University of New York In.

Maier, J., Padmos, A., Bargh, M. S., & Wolfgang, W. (2017). Influence of Mental Models on the Design of Cyber Security Dashboards. In *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP)* (pp. 978–989). https://doi.org/10.5220/0006170901280139

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computer & Security*, *31*(4), 1–44.

Volkamer, M., & Renaud, K. (2013). Mental Models — General Introduction and Review of their Application to Human-Centred Security. *Number Theory and Cryptography. Springer, Berlin.*

Wash, R., & Rader, E. (2011). Influencing Mental Models of Security : A Research Agenda. In *Proceedings of the 2011 New Security Paradigms Workshop ACM*.

Wilson, J. R., & Rutherford, A. (1989). Mental Models : Theory and Application in Human Factors. *Human Factors*, *31*(6), 617–634.

Xie, B., Zhou, J., & Wang, H. (2017). How Influential Are Mental Models on Interaction Performance ? Exploring the Gap between Users ' and Designers ' Mental Models through a New Quantitative Method. *Advances in Human-Computer Interaction*.