Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 8, Issue. 1, January 2019, pg.105 – 118

YOUTH'S ATTITUDE TOWARDS INTERNET CRIME: SOCIAL FACTORS, CAUSES AND EFFECTS

[1]Gbenga T. Omoniyi; [2]Shahrudin Awang Nor; [3]Nor Iadah Yusop; [4]Rotimi-Williams Bello

[1]Awang Had Salleh Graduate School, UUM College of Arts & Sciences, Universiti Utara Malaysia
[2]SETARA, PPPM (PT) & Rating Manager, Strategy Planning Division, Institute of Quality Management, Universiti Utara Malaysia
[3]School of Computing, UUM College of Arts & Sciences, Universiti Utara Malaysia
[4]Department of Mathematical Sciences, University of Africa, Toru-Orua, Bayelsa State, Nigeria
Email addresses: [1] geegartea@yahoo.com, [2] shah@uum.edu.my, [3] noriadah@uum.edu.my, [4] sirbrw@yahoo.com

Abstract: Computer crime, also commonly referred to as Internet or online crime is any type of crime scheme that uses one or more components of the Internet to commit a criminal act. Agreeably, the Internet technology has influenced productivity and connectivity among people. This is not without some security challenges that threaten the users of the Internet. The level at which these security challenges threaten both the citizenry and the government of Nigeria is alarming. This implies that Internet crime in Nigeria is societal menace and questions on the factors enabling the rampant of Internet crime among the youth in Nigeria must be asked. The objective of this paper is to address the social factors, causes and the effects of youth's attitude towards Internet crime. As such, 130 Internet users from universities were surveyed using self-administered questionnaires distributed across Lagos state, Nigeria. The data collected through survey and questionnaire was analyzed using analytical techniques such as Pearson correlation and hierarchical regression. Based on the findings of this study, it can be concluded that there is significant effect of age, sex, belief, knowledge, commitment, and involvement factors on the youth involvement in Internet crime in Nigeria. However, security policy severity, security policy certainty, attachment, and attitude did not have significant effect on youth involvement in Internet crime in Nigeria.

Keywords: Questionnaire; Internet crime; Criminal act; Youth; Pearson Correlation; Lagos state; Regression; Social factors

I. INTRODUCTION

The Internet is a massive, computer-linked network system used globally to access and convey information, either by personal or business computer users; it is also used for communication, research, entertainment, education and business transactions [1], [2]. Today, the Internet can link all online computers so that people can use it to communicate throughout the world [2]. Through Internet, computers around the world are connected by the use of a standard protocol. Internet crime can occur whenever any of the protocols used is compromised. Different cyber-attacks are made possible due to one or combination of the following: social engineering, parameters manipulation,

malware, pharming, SQL injection, spoofing, phishing, Bruteforce attacks, weak password, website defacement, use of unpatched software, organized crime syndicates, physical disconnection, and internal security breaches among others. Among the criminal activities that are committed on the Internet, greater percentage goes to the youth. This is in line with the findings of [3] as well as [4] who revealed the possibility of a variety of factors to predict attitudes to corruption.

Similarly, people with high scores in need for achievement have been found to be characterized by a tendency to seek challenges and a high degree of independence. [5] added that the most satisfying reward of people with high need for achievement is the recognition of their achievements. These are not unconnected with the changing in the value system of Nigerians. Achievement in terms of material wealth has taken a centre stage in every facet of our lives [6]. A society where need for achievement significantly predicts youth involvement in Internet crime needs to do value re-orientation, at least to safe her existence. [7] examined secondary school students' perceptions of incidences of Internet crime among school-age children in Oyo and Ondo states, Nigeria. The study indicated that students are being initiated into Internet crime by their friends in the universities, polytechnics, and colleges of education. Furthermore, male students are more involved than their female counterparts, a reflection of what happens worldwide. Also, senior secondary school students' involvement in Internet crime is not a function of the socioeconomic status of their parents, as students from both rich and poor homes engage in the crime. In addition to this, the involvement of students in Internet crime has no effect on their academic performance, as the students' higher level of cognitive thinking being used to scam people on the Internet is being exploited to enhance their academic standard. [8] contends that in Nigeria, unlike the traditional criminal groups, both sexes are functionally involved in Internet crime, with varying specialized functions. [9] and [10] claim that the anonymity and privacy that the Internet provides for potential users has excessively enhanced the degree of fluidity and structural complexity of the 'yahoo-boys' operations in Nigeria. Today, they get access to the Internet without leaving the home. Embezzlements, electronic crimes, fictitious sales of properties and cars are all being carried out without leaving a trace. Also, gender has emerged among the yahoo-boys in Nigeria. This is essentially for the purpose of facilitating their nefarious activities. At a single point in time, an individual could claim to be a "beautiful lady" or a "big man" or a "celebrity", all depending on his/her immediate needs.

This finding is in line with [11] who found out that men and women have different cultural orientations that may influence the way in which they define electronic communication situations. "Gender characteristics are a primary means by which we sort and define self and others. Sex attributes provide basic information about how to conduct interactions with others and how to organize social reality" [6]. The practical contribution of this research will be towards the general public of Internet users in Nigeria, knowing the vulnerability and understanding the risk involved in Internet service usage would help in taking necessary precautions. Furthermore, results achieved by this research would help the users of the Internet services to be protected in terms of the reduction or at the very least, managing Internet crime. Findings from this research would also help the regulatory agencies in charge of the Internet activities in Nigeria to decide the path to sail in winning the fight against Internet crime and protecting users by incorporating social factors in preventing Internet users against perpetrators of Internet crime. This study is also carried out to help both the practitioners and relevant regulatory bodies to have a better grasp of the Internet crime status in Nigeria, to understand what challenges users are facing in terms of curbing Internet attacks and the varieties of attacks Internet users have to deal with. The major influence of this research is the pioneering approach of understanding the role of social factors and how it influence Internet crime in the Nigeria cyberspace. The findings of this study would imply constructive recommendations to practitioners, stakeholders, policy makers and the general public on what to take serious in the course of managing Internet crime in the Nigerian cyber space.

II. METHODOLOGY

II.I Research Design

The study adopted theoretical perspectives of social cognitive theory in examining youth's attitude towards Internet crime. In addition to that, the data collected through survey and questionnaire was analyzed using analytical techniques such as Pearson correlation and hierarchical regression.

II.II Participants and Sample

Lagos state is selected as the only population of this study because it is considered a cosmopolitan state that house citizens originated from all the six regions of the country. More so, Lagos state has the highest population among Nigeria states. Using the G*Power Analysis [12] as shown in Fig. 2.1 to determine the sample size of the respondents of the study, 85 respondents are revealed to be the minimum sample size for this study. In order to maximize response rate, 85 is increased by 50%. Therefore, the sample size in this study is decided to be 130 Internet users. 130 Internet users were surveyed using self-administered questionnaires distributed across the different universities in the state. The decision to survey users from universities is because majority of Nigerian now have access to the Internet via various means such as, home, cyber cafés, free/paid Wi-Fi at school and other hotspot locations. And since tertiary institutions in Nigeria have mandated basic computer appreciation courses for all students (as well as inculcated it in all schools curriculum), also for the general knowledge that Nigerian students, lecturers and other citizens with basic computer knowledge have the tendency of surfing the Internet regularly for numerous reasons, there is high guarantee that all respondents encountered in the universities will be Internet users. Random sampling technique was also used in selecting the participants that eventually participated in the study.

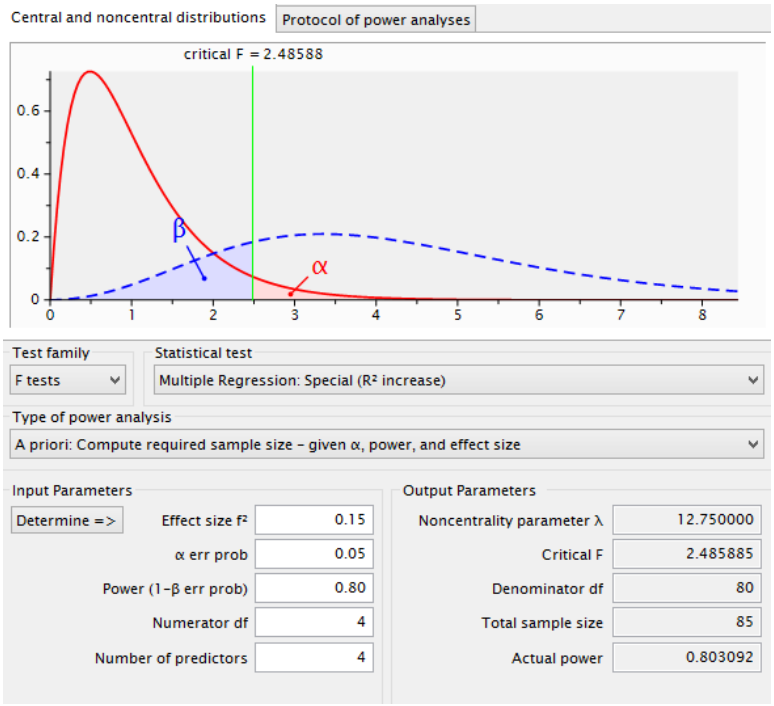

Figure 2.1: G*Power Analysis

II.III Instrument

[13], [14] have stressed the need for the design of research instrument in order to understand some underlying assumptions which help in formulating good questions that need to be answered by the participants. Redesigning research instrument for data collection is necessary in some cases that the previous and existing instruments are to be used in a scope that is different from previous research [15]. [15] argued that the object of study, research concept and dimensions require proper understanding before designing the research instrument. Thus, the researchers bear

the objective of research together with their dimensions and the participants in mind while designing the research instrument for this study. [16] asserted that structuring questionnaire in a manner that can be effortlessly comprehended and answered by the respondents is important as it affect the validity of the responses. If a questionnaire is structured well, respondent will be encouraged to answer the questions. Heedfully, in order to motivate respondents' response, the researchers clarified the objective of the research and guaranteed the respondents that their responses will be used anonymously and only for the purpose of the study. In line with this argument proffered by [17], stating it is important that researchers adhere to the research ethics by protecting the anonymity of their respondents and avoid ambiguous scaling of items. Therefore, the researchers ensure that the wordings of the questions are structured simplistically in order to maximize instruments' validity and reduce respondents' stress in answering the questions. Additionally, the questions were structured in a 5-point Likert psychometric scale for extracting the extent of agreement or disagreement of respondents to a certain statement in the questionnaire. The arrangement of the research instrument is sectioned into six parts. The first part entails questions on the background information of the respondents such as age, gender and their accessibility to Internet technology. The first section is followed by Section B and C which present items under severity and certainty of security policy respectively. Section D embodies items under the attachment. Section E presents items under commitment. Section F entails items measuring the involvement, section G is belief, section H is attitude, section I is knowledge and lastly section J entails items for Internet crime. The items were adopted from past studies and were adapted to suit the objective of this present research. For this study, a Cronbach Alpha reliability coefficient of 0.936 was however recorded.

II.IV Procedure

Figure 2.2 below depicts the procedure followed in this research in actualizing the survey research design.

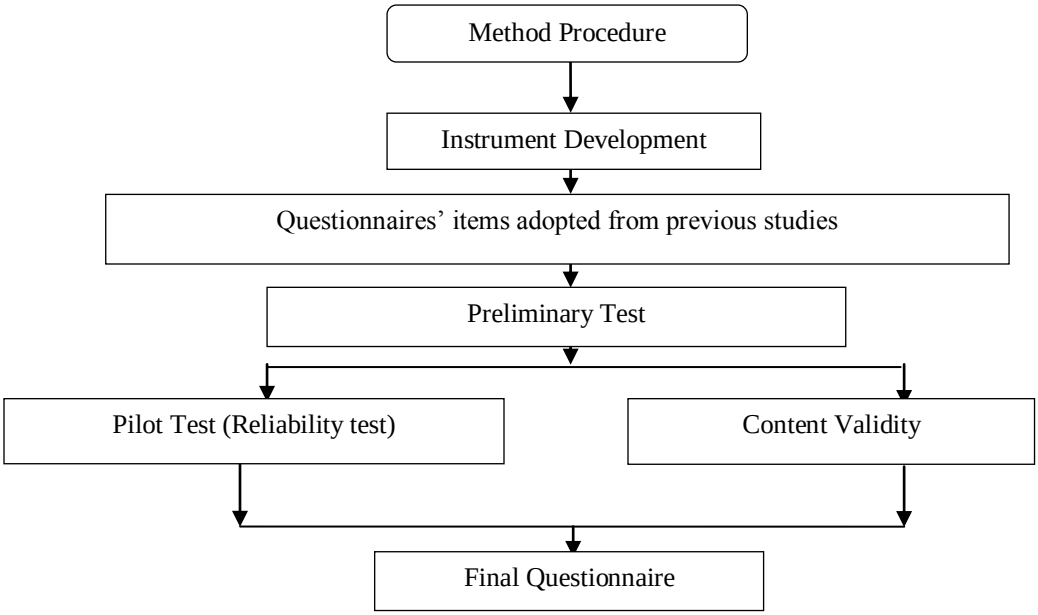

Figure 2.2: Survey design frameworks

This section highlights the respondent rate. A total number of 130 respondents were targeted and questionnaires were distributed to all of them, out of which 120 questionnaires were retrieved and 8 questionnaires were considered disqualified basically on the issue of incomplete fillings, high rate of missing responses to relevant questions and

similar issues, so, the overall valid retrieved questionnaires were 112 which was 93.33% usable for the purpose of the analysis. Table 2.1 shows the overall study survey response rate.

Table 2.1: Survey response rate

	Frequency	Percentage (%)
Questionnaire Distributed	130	100
Questionnaire Returned	120	92.31
Questionnaire Rejected	8	6.67
Questionnaire Retained	112	93.33

III. RESULTS AND DISCUSSION

Table 3.1: Multiple regression summary table showing relationship of each social factors on the level of youth's attitude towards internet crime

Model Summary[b]

Variables	Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
						R Square Change	F Change	df1	df2	Sig. F Change	
Security Policy Severity (SPS)	1	.551[a]	.303	.242	.941	.303	4.932	9	102	.000	1.670
Belief	2	.794[a]	.630	.443	.636	.381	3.362	37	110	.000	1.846
Security Policy Certainty (SPC)	3	.773[a]	.598	.394	.778	.293	2.929	37	110	.000	1.880
Attitude	4	.787[a]	.619	.426	.816	.619	2.929	37	110	.000	1.762
Attachment	5	.778[a]	.605	.405	.907	.619	3.023	37	110	.000	1.805
Knowledge	6	.737[a]	.543	.311	.839	.619	2.341	37	110	.001	1.841
Commitment	7	.734[a]	.539	.305	.892	.619	2.306	37	110	.001	1.704
Involvement	8	.778[a]	.606	.406	.885	.619	3.033	37	110	.000	1.659

a. Predictors: (Constant), SPS, Belief, SPC, Attitude, Attachment, Knowledge, Commitment, Involvement
b. Dependent Variable: IC3

Table 3.2: Anova results of all the predictors against level of Internet crime in Lagos state

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.324	9	4.369	4.932	.000[b]
	Residual	90.355	102	.886		
	Total	129.679	111			

a. Dependent Variable: IC3;
b. Predictors: (Constant), SPS, Belief, SPC, Attitude, Attachment, Knowledge, Commitment, Involvement.

From the results as shown in Table 2.1, the response rate is 93.33% of the returned questionnaire which is a good percentage of a survey data gathering. This indicates that the data will be able to provide a strong result and true picture of the study objective. The predictors or constructs of the study were tested for reliability and validity using Cronbach test (Table 3.4). The result as shown in the Table 3.4 indicates that all the measurement items are valid and significant as the values ranges between 0.722 to 0.825 values. It shows they are all significant and can really explain the variables to some degree of validity. The result shows that out of all the respondents of the survey, 51.8% of them are male compared to 48.2% that are female. The indication of the result is that more men get used to Internet among Nigerians. Male uses Internet facilities more than their female counterpart. It also indicates that they are more aware of Internet and its facilities and utilized it than their female counterpart.

This can also mean that men are more susceptible to Internet crime more than their women counterpart because they use Internet facilities more than the women in Nigeria settings. This result agrees with the findings of [18] and [19] where it was confirmed that male students are notably more participating than their female colleagues, an expression of what is happening globally. In addition, senior secondary school students participate in Internet crime not only as a result of the socio-economic significance of their parents but as students from both rich and poor homes engage in the crime.

Table 3.3: Coefficient results

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Co linearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	.880	.432		2.038	.044		
Security policy severity	-.006	.185	-.003	-.030	.976	.928	1.077
Belief	.322	.159	.303	2.028	.045	.306	3.267
Security policy certainty	-.259	.116	-.297	-2.235	.028	.388	2.576
Attitude	.160	.109	.162	1.463	.146	.558	1.793
Attachment	-.198	.246	-.069	-.805	.422	.931	1.074
Knowledge	-.328	.233	-.139	-1.411	.011	.703	1.422
Commitment	.564	.239	.224	2.361	.020	.757	1.321
Involvement	1.178	.227	.449	5.185	.000	.910	1.099

a. Dependent Variable: IC3

Table 3.4: Reliability measure

Constructs	Number of Items	Cronbach's Alpha
Security policy severity	4	0.947
Security policy certainty	4	0.804
Attachment	5	0.922
Commitment	3	0.811
Involvement	5	0.973

Belief	4	0.801
Attitude	5	0.944
Knowledge	7	0.825
Internet Crime	7	0.765

In term of age, among the respondents, those in the age bracket 19-24 years recorded 15.2 %. This is referred to as adolescence age that is still coming up into the reality of life and what it takes to cope with life. But there is a certainty that they will take after their senior in the age bracket 25-29 years and 30-39 years age bracket. Those in the age bracket 25-29 years came second with the percentage of 26.8. Looking critically at this, these are youth who are more versatile in the use of computers and Internet with the possibility of high involvement in cyber or Internet crime. The more they are exposed to Internet, the high the probability of getting involved in Internet crime and this reflect the good picture of what is happening in the country.

Age bracket 30-39 years has the highest percentage of 36.6. The indication of this is the fact that more youth of the country are exposed to Internet usage where they have access to online games, online betting, dating sites among others and thereby prone to Internet crime because of the JET (Junctional ectopic tachycardia) age syndrome. The age bracket of 40-45 years recorded 19.6% which is also higher and third in the rank. Lastly, those respondents in the age bracket of 60 years and above are least in the percentage value with 1.8 %. They are less prone to Internet crime because they rarely use Internet and computer facilities. This result corroborate the earlier findings in the literatures such as the one conducted by [7] where the views of secondary school students was observed on the frequency of the cyberspace crime among the school-age progenies in Oyo and Ondo states, Nigeria. The study shows that students are being lured into cyberspace scam by their associates in the higher institutions of learning [18].

From the regression analysis as shown in Table 3.1, the R^2 value is 0.303 (Adjusted R^2 is 0.242). This shows that the predictors or measurement variables, security policy severity, can only explain 24.2 % variance of the dependent variable, which is the level of Internet crime. Likewise, belief has R^2 = .630 and adjusted R^2 = .443. This means that this predictor, belief can only explain 44.3% of the dependent variable. In a like manner, the result of R^2 for security policy certainty as a predictor is .598 and the adjusted R^2 = .394.

Which means security policy certainty can only explain 39.4% of the dependent, the level of Internet crime. Meanwhile, attitude recorded R^2 = .619 and adjusted R^2 = .426, expressing that attitude only explain 42.6% of the dependent variable. As for attachment as a predictor has R^2 = .605 and the adjusted R^2 = .405, indicating that attachment can only explain 40.5% of the dependent variable. Knowledge recorded R^2 = .543 and the adjusted R^2 = .311. This signified that 31.1% of the dependent variable was explained by knowledge. In the meantime, commitment has R^2 = .539 and the adjusted R^2 = .305, this means, 30.5% of the dependent variable is explained by knowledge. Lastly, involvement has R^2 =.606 and adjusted R^2 = .406. It means involvement only explained 40.6% of the dependent variable. Using Table 3.3, the coefficient table shows the significant value, which represents the *P* value of each of the social factors.

Security policy severity has *P* =0.976 value. *P* = 0.976>0.05, so, it means it doesn't have a significant value to explain the variance of Internet crime. There is no significant relationship between security policy certainty and level of Internet crime in Nigeria. This actually indicates that the current security policy severity in Nigeria as it is being operated has no bite on the level of Internet crime. This result is in tune with the findings and suggestions of some researchers. [20] found the establishment of security policy to be significantly efficient in preventing the misuse behaviour of Internet by serving as a deterrent mechanism for trespassers. Similarly, [21] found security policy as a significant antecedent variable to Internet users' safety on the Internet. In line with this, [22] justified that the provision of stern security policy is part of the social factors that influence Internet crime in Nigeria. The study strongly recommended policy makers to enact stern policies that discourage the misuse behaviour of Internet technology and discourage Internet crime in Nigeria.

Belief recorded *P*= 0.045 significant value, *P* 0.045≤ 0.05, this is a little less or almost equal the standard hence it has significant value to explain Internet crime. It signifies that in Nigeria, the issue of belief in one faith or the other can influence the level of Internet crime. This corroborates the results of other researchers in which belief was expatiated as a factor that can influence level of Internet crime. For instance, [23] stated that belief, also known as personal norms denotes the workers' esteems and perspectives on information security conformity with organizational policies. [24] researched the role of belief in the development of appropriate computer behaviour. An appraisal of the study uncovered that belief influence people's disposition towards participating in organizational

information security misconduct [23]. It is guessed that people with good individual esteems and standards have an uplifting disposition towards agreeing to information security policies in organizations [23].

Security policy certainty is another social factor and it recorded a *P* value of .28 >0.05. This means this social factor is not significant in the context of Nigeria. The Nigeria level of Internet crime as at now and with the way and manner of the security policy and certainty has no influence on the Internet crime. It is not firmly enforced as expected. This finding is in tune with the findings by [24] which found no significant effect of security policy on users' misuse behaviour of the Internet. This was corroborated by [25] as he added in his suggestions that the lucidity and widespread promotion of security policies influence Internet users' adherence to security policies. In other words, enacting Internet security policies that protect Internet users is as important as making the policies accessible, understandable and comprehensible. Likewise, [26] established that agencies should also be responsible for making Internet users aware of the terms and conditions of security policies because users awareness of security policies determines their compliance and subsequently affect their safety and protection on the Internet.

Attitude has *P* =.146 and this *P* value > 0.05, indicating that attitude has nothing to do with the level of Internet crime in Nigeria context. The attitude of an individual, especially the Internet users' has no significant relationship with the level of Internet crime in Nigeria. Surprisingly, this is contrary to findings of a past study conducted by [27] where an empirical backing was given to this contention. This may be due to the nonchalant attitude of the Internet users to yield to the government policy severity and certainty.

Attachment is another social factor with *P* =.422 which is *P* value > 0.05, meaning that attachment has no significant relationship with the level of Internet crime in Nigeria. Attachment can be in various forms; the more attached an individual to their work schedule and organization policy, the lesser their attachments are to the Internet. This is according to past studies where it was explained by [28] that if a person feels attached to their organization more (and for the purpose of this study, Nigeria as a community); there is high tendency that they will not intend to get involved in any criminal activities. [24] argued that attachment can exist in different forms based on how the theory is intended to be applied, it could be parental attachment which involved being attached to one's parent, school attachment which involved being attached to one's academic institution, organizational attachment which involves being attached to one's place of work or community attachment which entails being attached to one's community as a whole.

Knowledge *P* value =.011 < 0.05. This simply means knowledge has a significant relationship with level of Internet crime. Most people or individual arrested for committing Internet crime are vast in Internet properties and facilities. They have the technical capacity and ability. This corroborates the findings of past study such as [29] which found a considerable relationship between knowledge, users experience and positive security behaviour of Internet users.

Commitment recorded *P*=.020 < .05 signifying that commitment has a strong significant relationship to the level of Internet crime in Nigeria. This may be as a result of the addiction syndrome of those that commit the crime in Nigeria society. This corroborates the findings and argument of past researchers like [28] which argued that if people are involved in conservative or socially accepted activities, they have a lower tendency of being engaged in any criminal activities because they will be too busy spending time with conventional people. [23] explains that individuals are the fundamental issue in the human parts of information security, because of their immediate contact with information. Their obligation and sense of duty regarding protecting information resources assume an imperative role in this aspect. While, in the word of [30], commitment denotes the desire to secure a high standard occupation. Individual accomplishment and status are quite essential to committed people.

Involvement has P=.000 which mean P < .05. This explained that involvement has a very strong relationship with level of Internet crime in Nigeria. This may be due to the fact that it takes involvement for such a crime to be committed. [31] describes involvement as creating or developing a good relationship with people or colleagues. [32] argues that involvement can be identified with costs of opportunity and how individuals invest their time. This result agreed with other research findings like [33] where it was demonstrated that the tie of involvement or participation such as attending informal meetings with people, creating personal relationships, being loyal and faithful to the organization and community are efficient in reducing computer abuse by the workers.

Therefore, it can be said that the hypothesis which stated that age, sex, belief, knowledge, commitment, and involvement factors will significantly, independently and jointly predict attitude towards internet crime among the youth in Lagos state was partially significantly supported by the study's findings.

IV. CONCLUSION AND RECOMMENDATION

Based on the findings of this study, it can be concluded that there is significant effect of age, sex, belief, knowledge, commitment, and involvement factors on the youth involvement in Internet crime in Lagos state and Nigeria as a whole. However, security policy severity, security policy certainty, attachment, and attitude did not have significant

effect on youth involvement in Internet crime in Lagos state and Nigeria as a whole. The following are the conclusion deduced from this research study:

(a) That male individual is more open to the use of computer set than female in Nigeria and hence more prone to Internet crime than their female counterpart.

(b) Those in the age bracket of 30-39 years are more users of computer set and Internet in Nigeria and they constitute the youth age of Nigeria.

(c) Majority of the respondents have computer set at home and have access to Internet facilities and broadband as well as fast speed Internet facilities.

(d) Most of social factors considered in this survey as measurement variables have low standard deviations that are values towards the mean of the set except for three of them which are security policy certainty-1.018, attachment-1.236 and commitment- 1.093 respectively.

Concerning their significances, involvement as a social factor has a strong significant relationship with the level of Internet crime in Nigeria. This is also followed by commitment, belief and knowledge. All these social factors contributed immensely to the level of Internet crime in Nigeria context. The social factors such as security policy severity, security policy certainty, attitude and attachment has no significant relationship with the level of Internet crime in Nigeria.

The researchers recommended that:

Government should concentrate more on the causes of youth's attitude towards Internet crime and its effects on the economy by putting in place policies and enlightening programmes on Internet usage in such a way that youth's life can be transformed so as to combat the social menace of Internet crime in Nigeria. Beyond that, the social menace which is the bane of Nigeria populace should be critically investigated and arrested than the way it is being handled currently, just as rightly presented by [22].

REFERENCES

[1] Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukopadhyay, T., Scherlis, W. (1998). Paradox: A social technology that reduces social involvement and psychological well-being? American Psychologist, 53, 1017–1031.

[2] Schneider, G. P., Evans, J., Pinard, K. T. (2006): The Internet Fourth Edition- Illustrated Introductory (4th Ed.). United States of America: Thomson CourseTechnology.

[3] Gbadamosi, G. and Bello, M. (2009) 'Profiling corruption perception in Africa: the role of religion, gender, education and age', in N. Delener, L. Fuxman, F.V. Lu, A. Putnova, and L.E. Rivera-Solis (eds) Proceedings of Business strategies and technological innovations for sustainable development: creating global prosperity for humanity conference, 7-11 July, 2009, Prague. Prague: Global Business and Technology Association (GBATA): 440-447.

[4] Treisman D. 2000. The causes of corruption: a cross-national study. Journal of Public Economics 76(3):399--458.

[5] McClelland, J. L., Rumelhart, D. E. (1981). An interactive activation model of context effects in letter perception: I. An account of basic findings. Psychological Review, 88(5), 375-407. http://dx.doi.org/10.1037/0033-295X.88.5.375.

[6] Fasanmi, S. S., Kaburuk, D. S., Ariyo, A. B. Influence of Psycho-social Factors on Youths' Attitude towards Internet Fraud in Nigeria. 4th WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES, WCETR2014. Procedia - Social and Behavioral Sciences 182 (2015) 110 – 115.

[7] Ige, O. A. (2008). Secondary School Students' Perceptions of Incidences of Internet Crimes among School Age Children in Oyo and Ondo States, Nigeria. A Master dissertation in the Department of Teacher Education, University of Ibadan.

[8] Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-boys sub-Culture in Nigeria. International Journal of Cyber Criminology, 2(2), 368–381.

[9] Reddick, R., King, E. (2000). The Online Student: Making the Grade on the Internet: Forth Worth: Harcourt Brace.

[10] Adeniran, A. (2006). A Non-Dependent Framework for Development, This day, www.thisdayonline.com

[11] O,Brien, J. (1999). Preface [to special section on NSCAT Validation and Science]. Journal of Geophysical Research 104: doi: 10.1029/1999JC900077. Issn: 0148-0227.

[12] Lyles, R. H., Lin, H. M., Williamson, J. M. (2007). A practical approach to computing power for generalized linear models with nominal, count, or ordinal responses. Statistics in Medicine, 26, 1632-1648.

[13] Daniel, M. (2012). Design Characteristics of Virtual Learning Environments: A Theoretical Integration and Empirical Test of Technology Acceptance and IS Success Research. Springer Gabler, Germany.

[14] David, C., Robert, W. C. (2007). Designing and Constructing Instruments for Social Research and Evaluation. John Wiley and Sons, Inc.

[15] Leiyu, S. (2008). Health Services Research Methods. 2nd Edition, Delmar learning, USA.

[16] Hair, J. F., Money, A. H., Samouel, P., Page, M. (2007). Research methods for business. Westsussex: John Wiley and Sons Ltd.

[17] Organ, D. W., Podsakoff, P. M., Mackenzie, S. B. (2006). Organizational citizenship behaviour: Its nature, antecedents and consequences. USA: Sage Publications, Inc.

[18] Greenberg, A., Hamliton, J., Maltz, D. A., Patel, D. (2009). The cost of a cloud: research problems in data center networks. ACM SIGCOMM Computer Communication Review, 39(1), 68-73.

[19] Gong, W., Li, Z. G., Stump, R. L. (2007). Global Internet Use and Access: Cultural Considerations. Asia Pacific Journal of Marketing and Logistics, 19(1), 57- 74.

[20] D'Arcy, J., Hovav, A., Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

[21] Haeussinger, F. J. Kranz, J. J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. International Conference on Information System 2013, 1-16.

[22] Odumesi, J. O. (2014). Combating the menace of cybercrime.International Journal of Computer Science and Mobile Computing, 3(6), 980-991.

[23] N. S. Safa, R.V. Solms, S. Furnell. Information security policy compliance model in organizations. Computers and Security, 56 (2006) 1-13.

[24] Lee, S. M., Lee, S. G., and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information Management, 41(6), 707-718.

[25] Siponen, M., Mahmood, M. A. Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? Communications of the ACM 52(12), 145-147.

[26] Herath, T., and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 1-12. Available from: http://www.swdsi.org/swdsi05/Proceedings05/paper_pdf/An%20Examination%20of

[27] Siponen, M., Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violations. MIS Quarterly 34(3), 487-502.

[28] Lee, J., Lee, Y. (2002). A holistic model of computer abuse within organizations. Information Management and Computer Security, 10(2), 57–63. https://doi.org/10.1108/09685220210424104

[29] Rhee, H. S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior, Computers and Security, 28(8), 1-11.

[30] Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers and Security, 39 (PART B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009

[31] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information and Management, 51(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

[32] Pratt, T. C., Franklin, T. W., Gau, J. M. (2008). Key Idea: Hirschi's Social Bond / Social Control Theory. Key Ideas in Criminology and Criminal Justice, (1969), 55–69. Retrieved from www.sagepub.com/upm-data/36812_5.pdf

[33] Theoharidou, M., Kokolakis, S., Karyda, M., Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers and Security, 24(6), 472–484. https://doi.org/10.1016/j.cose.2005.05.002

