SSRG International Journal of Humanities and Social Science
ISSN: 2394 – 2703 /doi:10.14445/23942703/IJHSS-V8I5P103

Volume 8 Issue 5, 14-22, Sep-Oct, 2021
©2021 Seventh Sense Research Group®

Original Article

Determinants of Cybercrime Awareness Among Internet users in Nigeria

Chibuike Ndubuisi Nwoke[1], Ogochukwu Favour Nzeakor[2], Nnamdi Green Nwoha[3], Obinna Ugwu[4], Osinachi Peter Uba-Uzoagwa[5] & Thank God Ikenegbu[6]

[1]*Department of Sociology & Anthropology, the Faculty of Social Sciences, University of Nigeria,*
[2&3]*Peace & Conflict Studies Unit, School of General Studies, Michael Okpara University of Agriculture, Umudike. Abia State, Nigeria,*
[4&5]*Social Science Unit, School of General Studies, University of Nigeria*
[6] *Institute of African Studies, University of Nigeria.*

Received Date: 02 August 2021
Revised Date: 03 September 2021
Accepted Date: 14 September 2021

Abstract - *The study used questionnaire, supplemented with IDI to collect data from 1,104 Internet users in order to examine the demographic and situational factors that influence the quality and/or volume of cyber-security awareness as a cyber-policing measure.*

Results: *1)Having falling victim of cyber-security incidents in the past significantly influences the volume and content of cyber-security awareness in the sense that more of the victims (M = 1.7, SD = 1.7) than non-victims (M = .73, SD = 1.3) of cybercrime were informed of cyber-security. 2)Educational level significantly influence awareness in the sense that more of the lowly educated (M = 1, SD = .9) than highly educated (M = .9, S.D = .8) Internet users were informed of cyber-security. 3)Marital status, age, and sex were not significant determinants of awareness, though it was shown that more of the ever married (M = 1.0; SD = .87), older (M = 1.2; SD = .86), and female (M = 1.1; SD = .88) Internet users were informed of cybercrime than their single (M = .98; SD = .88), younger (M = .96; SD = .88), and male (M = .88; SD = .87) counterparts. Increasing quality and proper awareness campaign was recommended.*

Keywords - *Awareness, Cyber-security, demographic factor, situational factor, victimization experiences*

I. INTRODUCTION

Increasing spate of cybercrime victimization is currently a huge source of concern for all and sundry. The concern is also exacerbated by the reality of increasing expansion of Internet connectivity; just as computer mediated communication is now a norm (Wall, 2010; Ndubueze, 2017; Rich, 2010). As a result, many users of Internet facilities are increasingly vulnerable to cyber security incidents. Though, the vulnerability of Internet users is due to many factors, but one of the most prominent factor is the fact that such Internet users in many cases are not aware of the risks of using the Internet, and often venture into cyber space vulnerably (Kritzinger & von Solms, 2010; Zhang et al., 2009; Liebel, 2013; Malby, Mace, Holterhof, Brown, Kascherus &Ignatuschtschenko, 2013; Liebel, 2013; Nzeakor, 2016; Nzeakor, Nwokeoma, & Ezeh, 2020).

Many a study have advanced the fact that cybercrime or information security awareness is one of the defences against continuously evolving threat landscape, and a way to mitigate security attacks (Siponen & Oinas-Kukkonen, 2007; Tsohou, et al., 2008; Aloul, 2012). It has equally been argued that despite the undertaken approaches and the use of security tools, humans remain the weakest link in information system security, with respect to the incidents they result to and the costs that are incurred (Aurigemma et at., 2012). In the same way, Joinson et al. (2010) found that despite the increasing level of penetration of technology in everyday life, individuals' behaviors with regard to protecting their own privacy have not progressed at the same pace. In this sense, cybercrime information security awareness enables a user to understand his/her role in the security process and encourages her/him to take necessary measures for his, as well as his peers' information security (Amankwa et al., 2014). It is therefore logical to assert that without increasing both the quality and volume of cyber-security awareness, there will be increase in cybercrime attacks and cyber-security incidents.

Meanwhile, a number of studies have been directed towards identifying both the factors and challenges of increasing cyber-security awareness. One of such factors as identified by Hansen (2007), Malby et al. (2013), Sasse, Brostoff and Weirich (2011), Leukfeldt et al. (2013), and Mylonas et al. (2013) is the issue of low prevalence or volume of cybercrime awareness. For instance, Mylonas et al., (2013) found that users of smartphones, one of the most commonly used ICT devices, lack security awareness and they are not adequately prepared to make appropriate security decisions. Leukfeldt et al. (2013), on their own, concluded that the first problem in detecting and investigating cybercrime in Singapore lies in the fact that victims of cybercrime don't always notice that they are being victimized.

However, other researchers like Utcu and Testik (2015), and Nzeakor et al. (2020) argued that the problem was more of quality or content, and less of volume of awareness. For instance, Nzeakor et al. (2020) found that though awareness level was relatively high in Nigeria, it was superficial in the sense that the Internet users were more aware of computer-assisted than computer-focused cybercrime categories. In the same token, Utcu and Testik (2015) argued that in certain instances, increasing awareness level has not corresponded with increasing relevant defensive behavior.

Apart from the factor of quality or content of cyber-security awareness, other studies have identified psychological, technical and economic factors to cyber-security or cybercrime awareness. Malby et al. (2013), in their study, discovered that despite a growing number of cybercrime awareness campaigns, a number of countries reported the view that it would take a while for the public awareness campaigns to build up the public trust; again, receipt of information about cybercrime did not necessarily translate into 'feeling informed' about cybercrime or cyber-security. The study also highlighted other challenges relating developing appropriate and cost-effective campaigns, providing information to users without additional training and skills acquisition activities. The study equally concluded that simple campaigns focused on a specific target group seemed to be most cost-effective. There are also limits as to how far users can be expected to learn complex security mechanisms, remember long and varied passwords for every online service they sign up to, and take other precautions that often directly interfere with the task at hand (Sasse, Brostoff & Weirich, 2001).

It is therefore glaring from the above that the knowledge of other factors like situational and socio-demographic factors influencing both the volume and quality of awareness of cyber-security or cybercrime awareness is still nascent. And understanding such factors will contribute immensely to the policies and interventions aimed at improving the quality and volume of cyber-security as a cyber-policing strategy.

A. Aim and objectives of the present study

The aim of the current study is to examine how demographic and situational factors influence the quality and/or volume of cyber-security awareness as a cyber-policing measure. The specific objectives are the following:

1. To find out the significant difference in participants' awareness scores based on their cybercrime victimization experiences.

2. To examine whether participants' awareness scores significantly differ on the basis of their marital status,

3. To ascertain the significant difference in the participants' awareness scores by their age.
4. To discover the statistically significant difference in awareness scores by gender.
5. To find out whether awareness scores of the participants significantly differ on the basis of educational level.

B. Research Hypotheses

1. Awareness scores of participants who have experienced cybercrime victimization are significantly higher than the scores of those who have not experienced cybercrime victimization.

II. LITERATURE REVIEW

As rightly observed by Zhang et al (2009), past research on information system (IS) or cyber-security awareness tend to lay less emphasis on the role of information security awareness in information system security or the control of cyber security incidents. The emphasis is rather more on end-user security; organizational factors and security behaviors together with user actions that influence the confidentiality, integrity, and availability of information system (Stanton et al., 2004); incorporating perceived technical security protection into the theory of planned behavior and examines factors affecting end-user security behaviors (Zhang et al., 2009); and others.

Apart from the above, other studies on information security or cybercrime awareness have emphasized psychological, technical and economic factors (see Malby et al., 2013; Sasse, Brostoff & Weirich, 2001; Rich, 2010; Hadlington, Binder & Stanulewicz, 2020). For instance, Hadlington, Binder and Stanulewicz (2020) examined the factor of "fear of Missing Out" in the prevalence of information security awareness; Malby et al. (2013) worked on the means and modes of carrying out effective anti-cybercrime awareness campaign; Sasse, Brostoff and Weirich (2001), Rich (2010), as well as AlMindeel and Martins (2020) concerned themselves with the inherent weaknesses with information security awareness dissemination; Gercke (2012), and Nzeakor, Nwokeoma and Ezeh (2020) examined the pattern or prevalence of cybercrime awareness; Leukfeldt et al. (2013) examined how lack of cybercrime awareness frustrates the efforts of criminal justice system in tackling cybercrime menace; Aydin and Chouseinoglou (2013) focused on fuzzy assessment of health information system users' security awareness; and Ogutcu and Aydin (2015) analyzed the personal information security behavior and awareness of information system users.

Stemming from the above, one obvious gap or limitation noticeable in the above reviewed literature is the fact that the demographic and situational factors influencing both the volume and quality of such cyber-security awareness are under-researched. Specifically, little is known on the factor of socio-demographic characteristics in the awareness of cyber security incidents. And fixing these gaps would help the stakeholders in fashioning suitable and effective awareness campaign that will eventual reduce the spate of cyber security incidents locally, regionally, and globally. For instance, while some authors like Sasse, Brostoff and Weirich (2011); Rich (2010); and others worked on the inherent weaknesses with information security awareness dissemination, lost sight of some socioeconomic, demographic, and situational factors that inform the quality of awareness assimilation and utilization. Malby et al. (2013), on their own, described the features of effective cybercrime awareness campaign at global level, however the focus was not on socio-demographic factors (p. 33). Again, while Hadlington, Binder and Stanulewicz (2020) linked low volume of information security or cybercrime awareness with increasing prevalence of "fear of Missing Out" among some selected employees in Saudi Arabia, has not brought to the fore other likely predicting factors like socio-demographic status; just as it seems doubtful that the phenomenon of "fear of Missing Out" affects the pattern of cybercrime awareness of wider population of Internet users, especially in Africa.

What is more, Ogutcu, and Aydin (2015), in analyzing the personal information security behavior and awareness of 881 information users, proposed four scales to measure how risky individuals' behavior is when using information system. They found that: the more the respondents perceive threats, their behavior becomes more protective; students, compared to other groups, are more vulnerable against risks; and that the education level and information security awareness are positively correlated (Ogutcu, and Aydin, 2015). However, this does not say much on other factors like sex, age, marital status and their relationship with cyber security incidents awareness

A. Theoretical Orientation

Trait Theories

Trait theories can be split into two major subdivisions: one that stresses psychological functioning and another that stresses biological makeup (biosocial theories) (Siegel, 2010). Among the major proponents are Anthony Walsh, Sigmund Freud, Alfred Adler, etc. (Aichorn, 1935). The major tenet of trait theories holds that "structure determines function". In this regard, how individuals are biological, socially, or psychologically structured determines how they function- including their awareness or cognitive level. Trait theorists today suggest that each offender is unique, physically and mentally; consequently, there must be different explanations for each person's behavior. Consequently, individuals' cyber-security awareness status may be explained differently based on some social, emotional, and situational configurations. However, trait theories have been challenged based on the fact that psycho-biological factors alone cannot trigger off behaviors- pro or anti-social behaviour.

III. RESEARCH METHOD

A. Study Design

The study adopted cross-sectional variant of survey design- using questionnaire as the main instrument of data collection, and supplemented it with In-depth Interview. The quantitative/questionnaire data measured/captured the factors influencing awareness of cyber-security; while the qualitative data exposed the dynamics of such influences.

B. Area and scope of the study

The area of the study was Umuahia North Local Government Area of Abia State. It is located within the coordinates of 5°32′N 7°29′E/5.533°N 7.483°E (Umuahia, 2017).

The scope of the study covered both structure and factors of cyber-security awareness of actual and potential Internet users residing in Umuahia Urban part of the Umuahia North LGA, Abia State during the period of the study- 2019 to 2020. Umuahia was justified as the study area on the strength that it is a state capital territory, and as such plays host, and even closer to some public, and financial institutions as well as other facilities that attract both cyber criminals and cybercrime victims alike.

C. Study Population

The target population of this study comprised of all potential and actual Internet users aged 20 to 70 years in Umuahia North Local Government Area of Abia State which was put at 223,134: with the male population as 112,595 (50.5%); and the female as 110,539 (49.5%) (National Population Census, 2006).

D. Sample Size

Sample size of 1,111 was initially selected based on published tables of sample (see appendix); however the sample size of 1,104 was actually selected based on the sampling procedure (see the section on sampling procedure below). According to Israel (1992, p.2), there are several approaches to determining sample size. These include using a census for small populations; imitating a sample size of similar studies; using published tables; and applying formulas to calculate a sample size. In this study, published tables were adopted (see appendix). According the published tables, under the error margin or desired level of precision of ± 3, any population size above 100,000 amounts to the sample size of 1,111; and recall that the population size of the area of the study was put at 223,134 (National Population Census, 2006). To supplement the quantitative data, a total of

12 participants- 2 persons per ward- were selected for In-depth interview.

E. Sampling Procedure

To obtain the study sample, probability sampling technique was adopted. In this sense, multistage cluster, systematic, and random sampling techniques were all adopted (Babbie, 2008, p. 228, & 233-234). At the first stage, the primary sampling unit, Umuahia Urban was clustered into 6 wards of: Ibeku East I, Ibeku East II, Ndume, Umuahia Urban I, Umuahia Urban II, and Umuahia Urban III**.** At the second stage, polling units, containing 148 housing units each in the 6 wards were listed, and systematic sampling technique with a random start was utilized in selecting 4 polling units each- totaling 24 polling units. Systematic randomization was used due to the availability of comprehensive sample frame (for details, see Nigeria Decide, 2019). In this sense, polling units in each ward were divided by 4, with a random start, in order to determine those elements/polling units that would be selected. In this sense, in Ibeku East I, every 4th polling unit (i.e., 17/4) was selected (more details are available on demand)**.** For Ndume, every 6thelement/polling unit (i.e., 22/4) was selected. In the case of Umuahia Urban I, every 9th polling unit (i.e. 37/4) was selected. For Umuahia Urban II, every 4th polling unit (i.e., 15/4) was selected. Finally, every 4th polling unit (i.e., 16/4) was also selected in Umuahia Urban III.

At the third stage, since there was no comprehensive list/sampling frame of both housing units and households, unlike in the preceding stages, random sampling technique was utilized in selecting 46 housing units from each of the 24 selected polling units- totaling 1,104 housing units. At the final stage, random sampling technique was equally utilized in selecting a respondent from each of the selected housing units until the 1,104 sample size was completed. Only housing units containing 2 or more respondents was qualified to be sampled.

Participants for the In-depth interview were selected based on the information from the retrieved questionnaire items. There was an appeal at the end of the questionnaire items that reads “Kindly drop your contact if you wouldn’t mind a further discussion of your experience(s) with the researcher”. Participants who complied were further ‘sifted’ on the grounds of number of time victimized, and their ward location- by so doing, 12 participants from the 6 wards were selected.

F. Data collection

I adopted questionnaire as the primary instrument, and In-depth interview guides as a supplementary instrument (see the appendices).

G. Data processing and analysis

The field data was analyzed using relevant descriptive and inferential statistics from the SPSS software version 23.

H. Ethical consideration

To guarantee the ethical considerations in research endeavor (i.e., principles of voluntary participation, no harm to the participants, anonymity and confidentiality-, and no deception) an introductory letters were attached to the questionnaire items and the interview schedules informing them of the purpose of the research, and their right of participation. They were also assured of the confidentiality, anonymity, as well as the commitment to use their data strictly for research purposes (see the appendices).

I. Participants

From the socio-demographic data, the result shows that more females (50.8) than males (49.2%); more single (62.8%) than married (37.2%) participated in the survey. Again, little above half (54.9%) of the participants were young; two-third (33.6%) were middle-aged; while very few (5.4%) of the old segment of the population participated. What is more, almost all the participants were Christians (98.5%); while other religious adherents like Islam, African Religion and Atheists rarely participated as they constituted less than 2%. For education categories, about 3 in every 5 participants (58.9%) were highly educated: constituting the modal education category. This was followed by 2 in 5 (40.5%) participants who were middle-educated; while very few of the lowly (.6%). Again, almost half of the participants (48.2%) were in working class group; followed by almost two-fifth (38.0%) who were students; with unemployed and self-employed being poorly represented as they were less that 10%.

J. Variable Definition

Cyber-security/cybercrime Awareness: In this study, it is operationalized as having appreciable knowledge of diverse criminal activities or computer security incidents on the Internet. To measure this, participants’ cybercrime/information security awareness status was elicited by asking the following questions in the questionnaire items: ‘Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM?’; ‘If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years’. Participants are regarded to be aware of cybercrime if they are able to mention or describe at least one category of cybercrime- say e-fraud; and this was coded as ‘1’ under the ‘value column’ in the row of ‘cybercrime status’ in the variable view of SPSS software (this is for categorical data). Again, any category of cybercrime mentioned attracted a score (1), and this was multiplied into the number of cybercrime categories mentioned for each participant (making up for scale data). On the other hand, they are regarded as not aware if they are not able to mention or describe any; and this was coded as

‘0’ under the ‘value column’ in the row of ‘cybercrime status’ in the variable view of SPSS software (for categorical data); and this was also scored as ‘0’ for a given participant (for the scale data).

Ever married participants: They are referred in this study as those who were either married, divorced, widowed or separated.

Highly Educated Participants: They are referred to those participants who have completed OND, NCE, B.Sc./HND and above.

Lowly Educated Participants: They are referred in this study as those participants who have completed secondary school and below.

Older Participants: They are referred in this study as those participants who aged 30 years and above.

Single participants: They are those participants who are yet to be married in any form.

Younger Participants: These refer to the participants whose age brackets fall below 30 years (age < 30).

IV. RESULTS

Objective one: To find out the statistically significant difference in participants’ awareness scores based on their cybercrime victimizstion experiences

To measure cyber-security awareness, questionnaire items No. 13 & 14 (Are you aware that people have been attacked, raped, or even lost money or lives through the Internet, phone, or ATM? If yes, please mention or describe the one(s) you are aware people have suffered on the Internet in last three years…) were used. A participant is regarded to be aware of cyber-security/cybercrime if he/she was able to mention or describe at least one of the cybercrime categories like e-fraud, hacking, etc. Again, question number “14”was correlated with that of No. 15 (Which of the following experience(s) have you had in the last 3 years? With the following options: My online account(s) (Eg.email, facebook, twitter, instagram, or bank mobile App) has been hacked; I have complied with strange email or call asking me to disclose my personal information, like password, or BVN; I have lost money to stranger I met online, or through phone/email; I have opened/replied spam mail(s); I have received email/text/call that threatened/insulted me; I have visited a stranger I met online and had an ugly experience; My computer/phone has been attacked by malware/virus; I have been contacted by criminal gangs to join them; etc). At this point, the difference in the awareness mean scores of participants who have been victimized of cybercrime and those who have not been victimized was measured.

As garnered from Table 1 (see appendix), the mean awareness scores (*M* = 1.7, *SD* = 1.7) of participants who have been victimized of cybercrime or cyber-security were more than the mean scores (*M* = .73, *SD* = 1.3) of those who have not been victimized. This difference was also significant *t*(1,103) = 7.550, *p* > .01; it also represented a medium-sized effect *r* = .51. This therefore means that cybercrime or cyber-security victimization influences awareness. In this sense, participants appear to be more aware of cybercrime than those who are yet to be victimized. This could also imply that individuals who have experienced certain cybercrime victimization experiences are more aware of such categories experienced than other categories yet to be experienced. It is also possible that their cyber-security victimization experiences preceded their awareness: they were not actually aware of cyber-security prior to their victimization experiences.

The pattern was also sustained by the IDI data. For instance, all the interviewed participants who admitted fallen victims of cybercrime, equally claimed that were well aware of cybercrime.

Objective two: To examine whether participants’ awareness score significantly differ on the basis of their marital status

Table 2 shows that the ever married were more informed (*M* = 1.0; *SD* = .87) of cyber-security than the single participants (*M* = .98; *SD* = .88). This difference was not significant, *f*(.110) = 1.612, *p* = .74; it also represented a small-sized effect *r* = .2.

Objective three: To ascertain the significant difference in the participants’ awareness scores by their age.

Table 3 : Independent samples t-test: Difference in the Awareness Scores of participants by their age

Cyber-security Awareness scores	N	Mean	SD	t-test	*P*
Younger participants	906	.96	.88		
Older participants	198	1.2	.86	-2.952	-

Note. p = .74.

Table 3 shows that older participants were more informed (*M* = 1.2; *SD* = .86) of cyber-security than the younger participants (*M* = .96; *SD* = .88). This difference was not significant, *t*(1,103) = -2.952 , *p = .38;* it also represented a small-sized effect *r* = .1.

Objective four: To discover the significant difference in awareness scores by gender

Table 4 : **Independent samples t-test: Difference in the Awareness Scores of participants by their gender**

Cyber-security Awareness scores	N	Mean	SD	t-test	*P*
Male	514	.88	.87		
Female	590	1.1	.88	-4. 079	**

Note. p = .52.

As garnered from Table 4, female participants were more informed (*M* = 1.1; *SD* = .88) of cyber-security than the male participants (*M* = .88; *SD* = .87). This difference was not significant, *t*(1,103) = -4.079 , *p = .52;* it also represented a small-sized effect *r* = .1.

Objective Five: To find out whether awareness scores of the participants significantly differ on the basis of educational level

Table 5 : Independent samples t-test: Difference in the Awareness Scores of participants by educational level

Cyber-security Awareness scores	N	Mean	SD	t-test	*P*
Highly Educated	632	.9	.8		
Lowly Educated	472	1	.9	. 936	*

Note. **p < .01, * p < .05.

As garnered from Table 5, the mean awareness scores (*M* = 1, *SD* = .9) of lowly educated participants were higher than the scores (*M* = .9, *S.D* = .8) of highly educated participants. This implies that more of lowly educated than highly educated participants were more informed of cyber-security incidents. This difference was also significant *t*(1,103) = .936, *p* > .05; it also represented a medium-sized effect *r* = .4

Hypothesis Testing

H_0: There is no statistically significant difference in the awareness scores of respondents who have experience cybercrime victimization and those who been victimized.

H_1: Awareness scores of participants who have experienced cybercrime victimization are significantly higher than the scores of those who have not experienced cybercrime victimization.

Test Statistics: Paired-samples t-test was adopted. To determine if a statistically significant difference exists among respondents' awareness scores, the variable was derived by scoring Internet users according to their scores in cyber-security awareness indexes (each index = 1 score); and those who did were not aware scored zero.

Level of significance: $p \leq 0.05$

Rejection Region

This was a one-tail, directional hypothesis where exact claim was made. If *p*> 0.05, the null hypothesis would be adopted suggesting that no significant differences exist; if *p*≤ 0.05, the substantive hypothesis would be adopted, thus suggesting that real difference exists between the awareness scores of participants who have experienced cybercrime victimization and those who have not.

Decision: results from *t*-test (see Table 1) indicate that on average, awareness scores (*M* = 1.7, *SD* = 1.7) of participants who have experienced cybercrime victimization are significantly higher than the scores of those who have not experienced cybercrime victimization (*M* = .73, *SD* = 1.3). This difference was also significant *t*(1,103) = 7.550, *p* > .01; it also represented a medium-sized effect *r* = .51. We therefore reject (H_0) and accept (H_1); and therefore conclude that Awareness scores of participants who have experienced cybercrime victimization are significantly higher than the scores of those who have not experienced cybercrime victimization.

V. DISCUSSION OF FINDINGS

The aim of the present study is to examine the demographic and situational factors that influence the quality and/or volume of cyber-security awareness as a mitigating measure to reducing cyber-security incidents in Abia State, Nigeria. This is aimed at closing some of the identified gaps in cyber-criminological literature. This was analysed under 5 specific objectives; including: to find out the significant difference in participants' awareness scores based on their cybercrime victimizstion experiences; to examine whether participants' awareness score significantly differ on the basis of their marital status; to ascertain the significant difference in the participants' awareness scores by their age; to discover the statistically significant difference in awareness scores by gender; and to find out whether awareness scores of the participants significantly differ on the basis of educational level. This led to the testing of a hypothesis. The findings emanating from the specific objectives are therefore discussed below:

From the objective one, we found that the mean awareness scores (*M* = 1.7, *SD* = 1.7) of participants who have been victimized of cybercrime or cyber-security were more than the mean scores (*M* = .73, *SD* = 1.3) of those who have not been victimized. This result corresponds with the result of the hypothesis which concluded that awareness scores of participants who have experienced cybercrime victimization are significantly higher than the scores of those who have not experienced cybercrime victimization. This implies that cybercrime or cyber-security victimization appears to significantly influence or determine volume or quality of cyber-security awareness. In this sense, individuals who have experienced certain cybercrime victimization may be more aware of such categories they experienced than other categories yet to be experienced. It is also possible that their cyber-security victimization experiences preceded their awareness: they were not actually aware of cyber-security prior to their victimization experiences. In line with studies like Hansen (2007), Malby et al. (2013), Sasse, Brostoff and Weirich (2011), Leukfeldt et al. (2013), and Mylonas et al. (2013) that reported a very low prevalence or volume of cybercrime awareness. This therefore means that there is actually very low volume of quality or adequate awareness of cybercrime/or cyber-security incidents.

The result equally supports and explains other findings like Joinson et al. (2010) who found that despite the increasing level of penetration of technology in everyday life, individuals' behaviors with regard to protecting their own privacy have not progressed at the same pace. This is because their awareness of cyber-security incidents is faulty, limited, and mostly concomitant on their cybercrime victimization experiences. The result could lead us into calibrating awareness into three: adequate /sufficient awareness; partial/superficial awareness; and naïve/zero awareness.

Sufficiently informed users, in this respect, are less likely to fall victims of cybercrime because they are more likely to be paranoid online; sufficiently abreast of the tricks of the cybercriminals and other cybercrime risk behaviours. Their awareness is less likely to be an offshoot of victimization experience, but rather of proper and formal users' education and guide.

Partial awareness should be the most prevalent of all the categories. However, while this category appear to be less likely to fall victims of cybercrime than the naïvely informed users; they are more likely to fall victims than the sufficiently informed users. Equally, it appears that this category of awareness is consequent upon and limited to those categories of cybercrime victimized of.

Zero awareness appears to be more prevalent than the sufficient awareness, and less prevalent than the shallow awareness. Meanwhile, this category appears to be most vulnerable to the cyber security incidents than the other categories- shallowly informed and sufficiently informed users. They mostly exhibit risky behavior online because their online behavior appears to be influenced by psychological factor- 'fear of missing out'. They are the bulk of "Jonny just come online". They are more likely to open improper and multiple online accounts without remembering their passwords- hence more susceptible to hackers and other online criminal activities.

This result is equally very striking when juxtaposed with other relevant findings. For instance, it gives credence and makes for dipper understanding of studies like Microsoft's Estimate (2014), Hansen (2007), Siegel (2010), Wall (2010), Malby et al. (2013), and Smartsev (2020) which reported a high spate of cybercrime or cyber-security incidents. For instance, Microsoft's Estimate (2014) reported that about one half of all adults connected to the Internet were victims of cybercrime. Just as Smartsev (2020) predicted that cybercrime crime will cost the world $11.4 million each minute in 2021. The increasing spate of cybercrime victimization therefore implies increasing awareness of such cyber-security incidents. However, it must be observed that increase in the volume of awareness is different in the increase in the quality or content of awareness. This is in concordance with Nzeakor, Nwokeoma, and Ezeh (2020) who concluded that though the level of cybercrime or cyber-security awareness was very high (89%); it appeared very superficial or limited because majority (78%) of the respondents tend to be only informed of certain categories (computer-related/assisted categories) of cybercrime or cyber-security incidents.

The above reality has therefore closed the gap in the situational factors of cyber-security of information security awareness. It should be therefore factored in any policy and intellectual intervention. This is because without increasing both the quality and volume of cyber-security awareness, there will be increase in cybercrime attacks and cyber-security incidents.

The results also show that ever married (*M* = 1.0; *SD* = .87), older (*M* = 1.2; *SD* = .86), and female (*M* = 1.1;

SD = .88) participants were more informed of cyber-security than their single (*M* = .98; *SD* = .88), younger (*M* = .96; *SD* = .88), and male (*M* = .88; *SD* = .87) counterparts. These results partly agree with Nzeakor, et al. (2020) who found that more males (91%) and older (97%) respondents tend to be more informed of cybercrime than their counterparts. More research is needed to unravel the discrepancy in the findings.

Finally, it was found that educational level appears to significantly influence awareness in the sense that more of lowly educated (*M* = 1, *SD* = .9) than highly educated participants (*M* = .9, *S.D* = .8) were more informed of cyber-security incidents, *t*(1,103) = 7.550, *p* > .01. The result implies that more of the lowly educated participants may have experienced cybercrime victimization than the highly educated participants as per the finding in objective one. However, the result contradicts that of Nzeakor, et al. (2020), and Ogutcu, and Aydin (2015) who found that the education level and information security awareness are positively correlated.

A. Conclusion

From the findings, we conclude that:

- Cybercrime victimization experience or having falling victim of cyber-security incidents in the past significantly influences/determine the volume and content of cyber-security awareness in the sense that more of victims than non-victims of cybercrime were informed of cyber-security.
- Educational level significantly influence awareness in the sense that more of lowly educated than highly educated Internet users were informed of cyber-security.
- Marital status, age, and sex were not significant determinants of awareness, though it was shown that more of the ever married, older, and female Internet users were informed of cybercrime than their counterparts.

These results have not only filled the gaps in the situational and demographic factors in the volume and content of cyber-security awareness; they have equally given deeper insights and credence to other studies like Nzeakor, et al. (2020), Microsoft's Estimate (2014), Hansen (2007), Siegel (2010), Wall (2010), Malby et al. (2013), Smartsev (2020), Joinson et al. (2010), Hansen (2007), Malby et al. (2013), Sasse, Brostoff and Weirich (2011), Leukfeldt et al. (2013), and Mylonas et al. (2013). The findings have revealed the dynamics, nature, and limitation of awareness as a cyber-policing strategy.

B. Relationship of the findings to the theoretical orientation

Trait theory was adopted to guide the study to understand how socioeconomic, environmental biological and personality forces combine to influence individuals' behavior like awareness of cyber-security. Trait theorists today suggest that each individual (offender or victim) is unique, physically and mentally; consequently, there must be different explanations for each person's behavior. Consequently, individuals' cyber-security awareness status may be explained differently based on some social, emotional, and situational configurations. And this understanding would ultimately reduce security incidents and criminality. The finding that victims of cybercrime, ever married, older, female, and lowly educated Internet users tend to be more informed of cybercrime or cyber-security incidents than the non-victims, single, younger, male, and highly educated users of Internet has justified the trait theory.

C. Contribution to Knowledge

Through this study, we aim to contribute to the better understanding of the situational and demographic factors or challenges of cyber-security or cybercrime awareness as a strategy of reducing the spate of cyber-security incidents. It is our belief that by discovering the situational and demographic factors and challenges of cyber-security awareness, interventions can be implemented to increase the volume and quality of awareness campaign that would lead to overall reduction in the spate of cyber security vulnerability. It would also help in strengthening and putting other relevant studies in proper perspective.

D. Future directions

From the developments from the current study, it would be revealing for future studies to focus on the structure, and categories of cyber-security awareness. Subjecting the three distinctions of awareness (adequate /sufficient awareness; partial/superficial awareness; and naïve/zero awareness) is equally worth substantiating empirically.

E. Recommendation

We recommend increased campaign of quality and proper awareness targeting all strata and demographic groups of the society.

Conflict of interest: The authors declare that they have no conflict of interest**.**

REFERENCES

[1] Aichorn, A. Wayward youth. New York: Viking Press(1935).

[2] AlMindeel, R. & Martins, J. T. (2020). Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. Information Technology & People (2020).

[3] Aloul, F. A. The need for effective information security awareness. Journal of Advances in Information Technology 3(3) (2012) 176–183. https://doi.org/10.4304/jait.3.3.176-183.

[4] Amankwa, E., Loock, M. & Kritzinger, E. A conceptual analysis of information security education, information security training and information security awareness definitions. In The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014) (2014) 248–252. IEEE.

[5] Aurigemma, S., Panko, R. R. (2012). A composite framework for behavioral compliance with information security policies. In: System Science (HICSS) 45th Hawaii International Conference on System Sciences. Maui, HI: 2012. p. 3248–57.

[6] Aydin, O. & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. Journal of Medical System, 37(6).

[7] Babbie, E. (2008). The basics of social research (4thed.). Belmont, USA: Thomson Wadsworth (2008).

[8] Boateng, R., Isabalija, R. S., Olumide, L., & Budu, J. Sakawa – Cybercrime and Criminality in Ghana. Journal of Information Technology Impact, 11(2) (2011) 85–100.

[9] Bringuel, A. & Rich, W. (2010). What role and responsibility does the government have in protecting consumer's rights to privacy/security on the internet? In & J. J. (T. Finnie, T. Petee (Ed.), Future challenges of cyber crime (2010) 47–50. Virginia: Futures Working Group.

[10] Chan, M., Woon, I.., Kankanhalli, A. A. Perceptions of information security at the workplace: linking information security climate to compliant behavior. J Inf Priv Secur. 1(3) (2005) 18–41.

[11] Fadilpasic, S. Cybercrime costing businesses millions every minute. Retrieved from https://informationsecurity.report (2019).

[12] Fitzgerald, J. D., & Cox, S. M. (2002). Research methods and statistics in criminal justice: An introduction (3rded.). Belmont: Wadsworth Thomson Learning.

[13] Gercke, M. Understanding cybercrime: Phenomenon, challenge and legal response. Geneva: International Telecommunication Union (ITU) (2012).

[14] Hadlington, L., Binder, J., & Stanulewicz, N. Fear of missing out predicts employee information security awareness above personality traits, age, and gender. Cyberpsychology, Behavior, and Social Networking.ahead of print, (2020) http://doi.org/10.1089/cyber.2019.0703.

[15] Hansen, J. R. Cybercrime prevention. In C. B. R. J. K. O'Shea, J. Steete, J. R. Hansen & & T. Ralgh (Eds.), Cybercrime investigations: Bridging the gaps between security Professionals,law enforcements and prosecutors (2007). 261–283, New York: SynGressPublishing.

[16] Internet crime complaint centre (2010). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

[17] Internet crime complaint center (2016). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

[18] Internet crime complaint center (2018). Internet Crime Report. Retrieved from http://www.ic3.gov/media/annualreports.aspx.

[19] Israel, G. D. Sampling: The Evidence Of Extension Program Impact. Program Evaluation and Organizational Development, IFAS, University of Florida. PEOD-6 (1992).

[20] Janczewski, L. J., & Xinli, S. F. Development of information security baselines for healthcare information systems in New Zealand. Computers & Security 21(2) (2002) 172–192.

[21] Joinson, A. N., Reips, U., Buchanan, T., & Paine Schofield, C. Privacy, trust, and self-disclosure online. Human-Computer Interaction, 25 (1) (2010).

[22] Mylonas, A., Kastania, K., Gritzalis, D. Delegate the smartphone user? Security wareness in smartphone platform. Computer & Security, 34(2013).

[23] Kazeem, Y. The FBI's Nigerian email scam ring bust shows how the billion-dollar global fraud has evolved. (2019) Retrieved from www.quartzAfrica.com

[24] Kim, E. B. Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1) (2014) 115–126.

[25] Kritzinger, E, & von Solms, S.H. Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security 29(8) (2010) 840-847.

[26] Lee, H. Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. International Journal of cyber Criminology, 12(1) (2018).

[27] Leukfeldt, R. 1., Veenstra, S., & Stol, W. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology, 7(1) (2013) 1–17.

[28] Liebel, D. The watch dog: Do you know the superagency that can best protect you from cybercrimes? (2013) Retrieved from http://www.dallasnews.com

[29] Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime, (February), (2013) 1–320. https://doi.org/10.1103/PhysRevLett.105.018904

[30] Mali, P. Cyber law consulting: Text book of cybercrime and penalties. (2008) Retrieved from www.cyberlawconsulting.com.

[31] Microsoft's estimate. About one half of all adults connected to the Internet were victims of cybercrime (2014). Retrieved from https://news.micrsoft.com/stories/cybercrime/

[32] Moulton, E. The future of cybercrime. In T. Finnie, T. Petee, & J. Jarvis (Eds), Future challenges of cybercrime (2010) 74-76, Virginia: Futures Working Group.

[33] National Population Commission. Population and housing census of the Federal Republic of Nigeria: Priority table. 1(2006) Retrieved from www.population.gov.ng.

[34] Ndubueze, P. N. (Ed.). Cyber criminology and technology-assisted crime control: A reader. Kaduna, Nigeria: Ahmadu Bello University Press Limited (2017).

[35] Nzeakor, O. F. Awareness of cyber policing among tertiary institutions in Imo State. An M.Sc thesis presented to the department of Sociology and Anthropology, University of Nigeria, Nsukka (2016).

[36] Nzeakor, O. F., Nwokeoma, B. N., & Ezeh, P-J. Pattern of cybercrime awareness in Imo State, Nigeria: An empirical assessment. International Journal for Cyber criminology, 14(1) (2020). Retrieved from http://www.cybercrimejournal.com.

[37] Obikeze, D. S. Methods of data analysis in the social and behavioral sciences. Enugu: Auto-Century Publishing. (1990)

[38] Ogutcu, G., Testik, O. M.., Chouseinoglou, O. Analysis of personal information security behavior and awareness. Computer & Security, (2015)56.

[39] Rich, W. Seniors and cyber space. In T. Finnie, T. Petee, & J. Jarvis (Eds), Future challenges of cybercrime(59-60). Virginia: Futures Working Group (2010).

[40] Sasse, M. A., Brostoff , S., & Weirich, D. Transforming the 'weakest link' - a human/computer Interaction approach to usable and effective security. BT Technology Journal, 19(3) (2001) 122-131.

[41] Shiloh, J. & Fassassi, A. Cybercrime in Africa: Facts and figures. Retrieved from SciDev.Net Sub-Saharan Africa.html. (2019).

[42] Siegel, L. J. Criminology: Theories, patterns, and typologies (10th ed.). Belmont, USA: Wadsworth Cengage Learning (2010).

[43] Siponen, M..T., & Oinas-Kukkonen, H. A review of information security issues and respective research contributions. ACM SIGMIS Database, 38(1) (2007) 60.

[44] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. Analysis of end user security behaviors. Computers and Security, 24(2) (2005) 124–133.

[45] The current state of cybercrime. An inside look at the changing threat landscape. Retrieved from http:// www.rsa.com. (2013)

[46] Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. Investigating Information Security Awareness: Research and Practice Gaps. Information Security Journal: A Global Perspective, 17(5–6) (2008) 207–227.

[47] Umuahia. (2017). Retrieved from https://en.m.wikipedia.org/wiki/Umuahia

[48] Utcu, G O., & Testik, O. M. (2015). Analysis of personal information security behavior and awareness. Journal of Computers & Security. Retrieved from: www.sciencedirect.com.

[49] Wall, D. S. Foreword. In K. Jaishankar (Ed.). Cyber criminology: Exploring Internet crimes and criminal behavior. London: CRC Press (2010).

[50] Zhang, J., Reithel, B. J., Li H. Impact of perceived technical protection on security behaviors. Inf Manag Comput Secur;17(4) (2009) 330–40.