INTERNATIONAL JOURNAL OF SOFT COMPUTING

MEDWELL PUBLICATIONS

Adventurism, Information Technology Self-Efficacy and Age as Predictors of Cybercrime among University Undergraduates

Nwabueze Cletus Offor
Department of Psychology, Imo State University, Owerri, Nigeria

Key words: Adventurism, information technology, age, cybercrime, predictors

Corresponding Author:
Nwabueze Cletus Offor
Department of Psychology, Imo State University, Owerri, Nigeria

Page No.: 9-19
Volume: 16, Issue 1, 2021
ISSN: 1816-9503
International Journal of Soft Computing

Abstract: The study investigated adventurism, information technology self-efficacy and age as predictors of cybercrime among undergraduates of Imo State University. Three hypothesis were postulated and tested. Two hundred participants were selected from four student hostel alliances: Bishop's Court Hostel Alliance, Front Gate Hostel Alliance, Aladinma Hostel Alliance and Amawire Hostel Alliances using simple random and convenience sampling techniques. Their age ranged between 18 and 30 years with a mean age of 24.80 and a standard deviation of 2.96. Three instruments; Information Technology Self-Efficacy scale, Adventurism Scale and Cybercrime scale were used to collect data for the study. Data on age was collected using the personal data column on the instruments. The design of the study was cross-sectional survey design while multiple regression statistics was used to analyze the data. The results showed that adventurism and information technology self-efficacy significantly and inversely predict cybercrime while age directly and significantly predicts cyber crime. The result equally revealed that jointly adventurism, information technology self-efficacy and age also significantly predict cybercrime. Based on these findings, the significance of the study is that parents and education authorities should intensify efforts on ethical training and moral guidance to youths concerning their exploration with computer and internet services. The researcher recommends that government and corporate institutions need to increase enlightenment on the dangers of involvement in cybercrime to youth development.

INTRODUCTION

Background to the study: Today, we live in a digital world governed by cyber technology in which virtually every aspect of human activities is controlled by computer and the internet. These ranges from education, banking and finance, health, transportation, even agriculture is also receiving a heavy dose of the cyber dynamics, especially in the more advanced and developed countries. The contemporary world is becoming a frenzy society in

which the fantasy of dream is ostensibly turning into reality and everybody is struggling to catch up. Computer and the internet have indeed revolutionized the world and appear to make life much better than the jet age of the antecedent civilization. The World Wide Web (WWW) was first invented in 1989 while the first ever website was created in 1991. Presently, there are about 1.9 billion websites with about 4 billion internet users. In other words, nearly half of the world population of 7.7 billion people are currently connected through the internet.

Household equipment ranging from refrigerators, ovens, air conditioners, television networks, radios; office equipments-printers, telephones; industrial machines, installations and equipments, etc. are controlled by computers and can be purchased and operated through the internet, thus, making life much easier and luxurious.

Life, however is an opportunity cost. The efficiency and glory of computer and the internet world is not devoid of the nefarious behaviour of men of the underworld whose activities today are severely threatening the fabrics of the beauty of the present generation, through cyber crime. Shinder[1] defined cybercrime as any criminal offence committed using internet or computer or computer network as the crime. It is offence committed against individuals or group with a criminal motive of intentionally harming the victim or causing physical, economic or mental injury to the victim directly or indirectly using modem communication network such as internet or mobile phone. Wikipedia defined it as illegal internet mediated activities that often take place in global electronic networks. Wall also perceives it as crime involving a computer and network in which computer may be used in the commission of the crime or may be the target of the criminal behaviour. It poses a threat to a person or nation's security and financial health. According to Cyber Security Ventures, cybercrime is perhaps one of the greatest threat to every contemporary company in our present world or indeed one of the greatest problems of mankind globally. In 2014, cybercrime was estimated to have cost the world's economy about $500 billion or about 0.70 of global income generally. At present cybercrime is estimated to cost the world about $600 billion or 0.80% of overall GDP and the reasons may include quick adoption of new technologies by cybercriminals, the increased number of new internet online users, especially from low income countries and the increased ease of committing cybercrimes without being apprehended due to growth of cybercrime-as-a-service. Cybercrime apparently ranks third in dollars in terms of most expensive crimes in the world, narrowly trailing behind government corruption and narcotic crimes. Its superiority over other crimes lies in its powers of affecting millions of people at specific times. According to Pew Research Center over 64% of Americans had been victims of fraudulent charges or loss of personal information.

Cybercrime exist in different forms such as identity theft, desktop counterfeiting, internet chat room, cyber harassment, fraudulent electronic mail, Automated Teller machine spoofing, pornography, piracy, hacking, phishing, spamming, etc.[2]. Ribadu identified prominent forms of cybercrime in Nigeria as cloning of web site, false representation impersonation, internet purchase and other kinds of frauds. While Olugbodi identified cybercrime as web site cloning, financial frauds, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mail, cyber laundering, virus/worm/Trojan, etc. Omodunbi *et al*.[3] listed Bank Verification Number (BVN) scams in Nigeria, theft of bank cards, phishing, software piracy, Data and Airtime (DAT) theft, Sales fraud and forgery, cyber plagiarism, cyber pornography, Nigeria Prince (beneficiary of a will) scam, Charity fund raising, cyber stalking, harassment and blackmail, social hijacking, etc. as some of the common cyber criminal activities going on in Nigeria.

Others include subscription fraud, WannaCry ransomware, etc. Subscription fraud occur when an individual applies and obtains a wireless telephone account using counterfeit or stolen credit card or account number or a stolen means of identification. Means of identification entails the use of another person's credit card number instead of the plastic card itself. It involves devices such as International passports, birth certificates, driver's licenses, social security numbers (e.g., user ID or passport) and unique biometric data such as fingerprint, voiceprint, retina or iris images.

Cloning is the theft of an Electronic Serial Number (ESN) and a Mobile Identity Number (MIN) assigned to a legitimate wireless phone and the installing these numbers on a stolen phone. Once installed, the cloned phone numbers behaves exactly like the phone owned by the legitimate customer. The cloned number is then used to access the internet to harm the owner.

Research has shown that cybercrime is not restricted to individual criminals, Group of people, firms and even corporate organization, authorities and government of nations at specific times get deeply involved in cyber criminalities for specific reasons. The first person ever to be convicted of cybercrime is Ian Murphy, popularly known as Captain Zap, in 1981. He hacked into American telephone company to manipulate the internal clock so that users can still make free calls at pick times (goosevpn.com). Ever since then, cyber crime has grown in bits and bounds in complexity and sophistication across the globe, affecting billions of people and business organizations.

Other individual apprehended for apprehended in cyber crime include Lennon Ray Brown. He was a computer engineer at citibank Regent Campus in Irving Texas. Out of vengeance over perceived management's attempt to fire him, he wiped out the company's entire account system, simply by transmitting a code and command to 10 core city bank Global control center routers which wiped out connectivity to networks, short down 90% of firm's network across America)[4].

Yet, others culprits include Ryan Cleary, aged 19 years who distributed DOS attack on British service Organized Crime Agency (SOCA) in 2011 and the website of International Federation of Phenographical industry in 2000. He was also accused of hacking into the website of another under group and exposed over 600 nicknames and IP addresses. The group consequently revenged against him by providing the link for his apprehension by the security agents[5].

Andrew Auernheimer, was a 25 years old who hacked into the website of the American Telephone company (AT and T) in June, 2010 and obtained the email of about 114,000 iPad users, specifically celebrities and politicians. He later sold the stolen information to a criminal group named Gawker media who used them for cyber criminal activities[5].

Also another 24 years old Aaron Swartz, in 2012, downloaded >4 million academic articles through (MIT) network connected to JASTOR (an academic online repository). He was discovered to be a 'freedom of information activist who advocated for civil disobedience against copyright laws that prevented people from gaining access to publicly funded research. His intention, according security report was to distribute the articles freely to all persons he believed may need them[5, 6].

Christopher Chaney was a 35 years man, who used information he obtained from celebrity blog sites, to guess the password of Google and Yahoo account of over 50 star celebrities. He hacked into these celebrity's accounts and set up an email forwarding system which sent himself a copy of all email posted to the stars. Within a year period, he had access to emails, photos and confidential documents of the stars. He was accused of being responsible for releasing and uploading the nude photos of Scarlett Johanson into the internet in 2010. He was later arrested and charged for voyeurism[7].

Clandestine group are not left out of cyber criminality. For instance, Dreamboard is an underground cyber group in United State of America which has a network of other cyber criminal members across the globe. They engaged in exchange of illicit images of children under the age 12 years. Their objective was described as sexual gratification through competition.

Darkmarket has over 2500 members across the world, including Canada, UK, USA, Russia, Germany, France, Turkey. It was a group platform for buying and selling credit card and bank information obtained through fraudulent ways. The group was highly organized, structured and apparently secured. The motive behind their activities include seeking for recognition and status through self enrichment[8, 9].

Another group named DSNChanger was made of a group of six men from Estonia, aged 26-31 years who stool advertising views and operated a DNS Changer malware which allowed them to control Domian system DSN servers. About four million computers were infected by the malicious malware. The group made about 14 million dollars before they were apprehended[10].

DrinkOrDie was also another group of software pirates formed in Moscow in 1993. It eventually expanded to 65 members in 12 countries: Britain, Australia, Finland, Norway, Sweden and USA. Members included university undergraduates and IT professionals, technically sophisticated and skilled in security programming and internet communication. Their activities include reproducing pirated copies of software, games, movies, etc., of genuine company products and distributing them before their formal introduction into the market by the copyright company. For instance, Window 95 was reproduced and distributed by the clandestine group two weeks before being officially released by Microsoft. The motive behind the group activities was to prove superiority as the first to release pirated version of any software. The new version of the product they pirated were usually obtained from employees of the copyright company[5].

Carberp was a malicious software designed in 2009 to steal banking information by a small closed group in Russian speaking countries, led by two brothers, slightly above 20 years of age. By 2011, the software was sold in other former Soviet societies. With the stolen information, the group transferred money from their victim's account into accounts controlled by the group members who withdraw the money using ATMs around the Moscow areas. They earned about two million dollars before they were arrested. However, despite the apprehension of the group members, Carberp continued to exist because the group had worked with three other cyber under-group criminals with whom a second version of the software was developed in 2010. Carberp was indeed perceived to be more effective and dangerous than Zeus and SpyEye with improved version still expected in due course which would obviously target markets in USA and Australia[11].

Unlimited operation: As a group, the inventor hacked into computer network of global financial institutions to

steal prepaid debit card data. They usually managed to eliminate card withdrawal limits of the ATM cards and withdrew money from ATM machines around the world. Members of the group were all US citizens, aged 25 years. These New York gangsters executed two major operations before they were arrested. In their first operation, they withdrew over $50 million dollars from 140 ATM machines in 20 countries and stole $400,000 in just two hour thirty minutes. In the second operation that lasted for 10 h, over $140 million were withdrawn from 3000 ATM machines[12]. The motive behind the group activities was criminal economic enrichment.

Koobforce was a worm-based malware created and targeted at web 2.0 social networks such as Facebook, Google, etc. It directs recipients to a fake website which requires them to download the unsuspected malware as updates of Adobe Flash Player. Once installed, Koobface controls the computer search engine and direct users to Koobface websites which was offering various scams such as fake investments, fake AV programs, fake dating services. The criminals made money through 'pay-per installed' and 'pay-per-click'. Five Koobface gang members, referred as 'Alibaba and 4' operated from Russia and Czech Republic. Some members of the gang had earlier worked in online pornographic and Spyware firms and attempted running legitimate mobile software and service business called 'Mobsoft Ltd' but failed. They earned about $2 million yearly before they were arrested. The motive of the group was purely economic and financial enrichment.

Beyond these and other individuals and criminal groups, nations and government agencies have also severally been accused of involvement in cyber crime or cyber espionage. For instance, the WannaCry ransomware attacks of 2017 targeted computers which run on Microsoft window operating system. It was a crytoworm that run on EternalBlue, an exploit of the US National Intelligence Agency (NSA) for older computer system. Before the breach was discovered, it was released by The Shadow Brokers, few months to the attack. WannaCry attack was reported to have affected about 200,000 computers in about 150 countries with the total damages ranging from hundreds of millions to billions of dollars. It was considered a network worm which included a transport mechanism that automatically scans for vulnerable computer systems and uses EternalBlue code to gain access into the victim. It uses the Double Pulsar tool to install and execute a copy of itself. EternalBlue code, however, is an exploit of US National Security Agency (NSA) developed for its own use when they noticed the internal vulnerability of Microsoft's Window's Server Message Block (SMB) protocol. Unfortunately they failed to notify Microsoft. Preliminary investigation by security experts suggested that WannaCry ransomware attack obviously originated from North Korea or its agencies in the country, who eventually stole the technology. The attacker displayed a payload information which kept informing the user that his/her files have been encrypted. Demand payment of about US S300 in bitcoin would be requested within 3 days or US S600 within 7 days or else several vital information would be wiped out their system. Three hardcoded bitcoin addresses or 'wallets were used to receive payments from victims. Such wallets, their transactions and balances were publicly accessible but the cryptocurrency wallet owners remained unknown.

According to Chatwin, in 2015, incoming mails of about 3 billion yahoo user's accounts were systematically scanned by US government with Yahoo's cooperation. Reuters News, also revealed that in 2016, Yahoo user's email were again accessed by US government through the FBI and the National Security Agency (NSA) who approached Yahoo to build a software program to read all user's incoming emails while searching for specific strings or digital signatures which are then copied and send to US intelligent agency server. The program spied on every one who emailed a Yahoo mail and therefore violated the privacy of people around the world. According to Chatwin, the NSA and FBI relied on section 702 of the Foreign Intelligence Surveillance Act (FISA), to justify their global top secret surveillance program and tracking foreign nationals and US citizens, an action which is unconstitutional and hence illegal. Yet Yahoo declined to challenge that sweeping order in court. The only action by Yahoo was to alert all users to change their password which is insufficient to protect user's safety.

Also, the Marriott hotel cyber attack report of 30th November, 2018 in USA affected about 500 million of its customers. The information accessed included payment information, customer name, mailing addresses, phone numbers, email addresses and passport numbers. According to CNN report, the attack was suspected to be the handiwork of Chinese Ministry of State security, being perhaps a prelude to the financial/trade dispute between USA and china.

The most serious problem, according to Edison Yu, an industrial manager at consultancy Frost and Sullivian USA is that cyber hackers are no longer interested in just stealing money but in stealing peripheral information such as contact detail and ID numbers that can be sold on the black market. According to him, global black market for email addresses and ID is now worth S500 billion dollars in black market[13].

Research have shown that some of the core forces or factors precipitating cyber crime include economic

benefits[5, 10-12, 14, 15], Intellectual challenge computer/ internet poses[16, 17], Desire to demonstrate technical proficiency[5], Competition[18], Protest[5,19], lust/pathology: voyeurism[5, 7], adventure. Others include widespread of online gaming, low average income of internet users and increases access to IT skills[20]. Omodunbi *et al*.[3] identified unemployment especially among teeming unemployed graduates, greed, incessant quest for quick wealth, lack of strong cyber crime laws and incompetent security on personal computers as other factors encouraging cyber crime in Nigeria.

In all situations, whether cyber crime is ascribed as individual, group, corporate enterprise or even government and its agencies oriented what is unobtrusive is that it is still people or individuals that are involved or used to precipitate it. While these studies have focused on specific actions involved or situational factors that precipitate cyber crime, relatively little research efforts have been devoted to the characteristics of the individual cyber crime offenders. This forms the first objective of the study.

This researcher therefore suspects that information technology self-efficacy may also play a significant role in attempts at cyber criminality. The information Technology Association of America (ITAA) defined Information Technology as the study, design, development, implementation, support or management of computer based information system, particularly software application and computer hardware. According to them, IT involves the use of electronic computers and computer hardware to convert, store, protect, process, transmit and securely retrieve information. In today's usage, IT encompasses all IC (Integrated circuit) electronic based devices, installations and equipment found in both giant macro mainframe computers, to micro devices found in PCs (Personal computers), telephone handsets and calculators. People are however not equally equipped to use IT gadgets, either because of its newness, sophistication, inexperience or outright fear of exposing their ignorance in a world that is consistently reverberating information technology. Expertise use of information technology to optimally achieve desired goals obviously rests on one's determination to learn and the confidence he has that he can do it. The later is succinctly captured in Bandura self-efficacy theory. According to Bandura, self-efficacy is one's confidence in his/her ability for doing something.

Bandura had proposed two types of the self-efficacy construct: the generalized and the specific self-efficacies. Generalized self-efficacy reflects the confidence one has in his ability to generally perform actions necessary to accomplish or attain desired goals or outcomes in a relatively wide range tasks. Specific self-efficacy, on the other hands, refers to one's confidence in his ability to perform specific actions, for attaining specific goals or outcomes. In other words, self-efficacy is a relative term. Information technology self-efficacy therefore is a domain specific aspect of the self-efficacy construct which defines one's belief and confidence in his ability to handle information technology gadgets, packages and facilities in order to accomplish IT related outcomes or attain specific goals on or with IT accessories. And this include the use of Microsoft Word, Access, Excel, Office Tool and homepages, the use of photocopying machines, fax machines, telephone handsets, calculators etc to produce and reproduce information technology-related tasks or attain certain IT goals or outcomes.

Most human behaviour are regulated by forethought which motivate people to behave in a proactive manner and engage in goal-setting efforts for personal or group accomplishments. This self-directedness is often propelled by self-reflective and self-reactive capabilities which are in constant interaction with environmental influences. Self-efficacy is therefore a dynamic concept often considered as an outcome of the process of evaluating, weighing and integrating information about one's capabilities and which in turn controls the choice one makes and the amount of effort he exerts on a given task.

In the same vein information technology self-efficacy therefore, refers to an individual's capability of using IT facilities to reach out and accomplish goals/targets. Consequently, people who experience or suffer pressure/stress from interpersonal contacts are bound to experience greater difficulties as a result of IT exposures or vice versa.

Since, it represents a cognitive valuation of oneself and ones abilities, researchers have wondered why it has not found as much application as similar concepts as perception, personality, expectation, motivation especially the process type such as the Expectancy theory of motivation, Equity theory or etc. These concepts are products of forethought which influence efforts or actions and are effectively utilized in industrial personnel activities.

One therefore, wonders why self-efficacy which is also a product of forethought, is under utilized in attempts at understanding human behaviour and activities including cyber criminality. This forms the second objective of this study.

Other variables which this researcher suspects as a precipitating factor to cyber criminality include adventurism. Adventurism is defined as improvising or experimentation in the absence or defiance of acceptable plans or principles willingness to take risk: actions or attitude regarded as reckless or potentially hazardous, a

willingness to take risk, especially in order to take unfair advantage in business or politics Collins Dictionary involvement in risky enterprise while disregarding established principles or adverse consequences[21].

No doubt, ability to handle and manipulate scenes, images and figures in the internet using computers produces an alluring and fascinating euphoria which creates nostalgic feelings that may also induce more desires to experimentations or exploring other available options. Though Wikipedia outlined adventure as one of the causes of cyber crime, relatively no empirical study has apparently been traced in literature on the impact on adventurism on cyber crime, hence, the third objective of this study.

Secondly, it appears that the categories of people that predominantly engage in cyber criminality are youth up to the age of 48 years. However, most studies on the relationship or impact of age on cyber criminal behavior have provided inconclusive findings. For instance, while Leonard *et al*.[22] found that age is not a significant factor in cyber crime, Gopal and Sanders[23] found that younger students were more likely to engage in cyber crime than older ones. Seale *et al*.[24] found that age is inversely related to the amount of cyber crime an individual commits while Cronan and Al-Rafee[25] found a direct relationship between the age of a person and the extent to which the person may engage in cyber crime. The inconclusive nature of these findings indicates needs for further research, hence this study. This forms the fourth objective of this study.

Theoretical review: Apparently, the theory of reasoned action and planned behavior by Ajzen and Fishbein[26] and Ajzen[27] appears to be the most relevant theory for explaining cyber criminality. The theory posits that the decision to engage in a particular behavior (Cyber crime) is the result of a rational process that is goal oriented and follows a logical sequence. Behavioural options are considered while consequences or outcomes of each are evaluated before a decision is reached to act or not. This decision is usually reflected in behavioural intentions which are often strong predictors of how well we will act in a given situation. According to the theory, intentions in turn are determined by two factors: attitude towards the behavior (cyber crime), i.e., people's positive or negative evaluation of committing cyber crime (whether it will yield positive or negative consequences) and subjective norm, i.e., people's perception of whether others will approve or disapprove any form of cyber criminality. According to Omodunbi *et al*.[3] one of the factors encouraging cyber criminality is relative lack of strong and effective laws regulating cyber crime in many countries, especially in developing economies of the world. Since, cyber crime occur across geographical or national boundaries, most cyber criminals therefore persist in their action knowing that they can acquire illicit money or wealth or harm people, organizations and even national interests without being apprehended can evade penal codes and escape punishment by the penal codes of many of the affected countries.

The theory of planned behavior which is essentially an extension of the theory of reasoned action) adds a third factor: perceived behavioural control. This reflects people's appraisal of their ability to perform the behavior (engage in cyber criminality), i.e., self-efficacy.

Empirical review: Though, a large number of studies reported about cyber crime focused on the forms, incidences and rates of cyber criminality across the globe, relatively little attention have been devoted to empirical research, nor on the personal characteristics of individuals involved in perpetuating cyber crime. In an analysis of the study of cybercrime among 600 student participants from four tertiary institutions in Ekiti State Nigeria, Omodunbi *et al*.[3] found that 98% of the participants have mobile phones and access the internet, 77% access Google, 82% access social media, 3.5% access academic research. The 9% of the participants use the internet for pornography, 31% use it for sports and games while 22% use it for piracy. The findings also revealed that participants who access pornography in the internet are also involved in piracy and spamming.

Choi *et al*.[28] reported that 60% of cyber security breaches occur from inside the organizations and are perpetuated by those authorized user inside the company. In their study of 185 participants from a large government transportation agency in Northeastern United States Metropolitan, the researchers found that user awareness of computer monitoring (UAC-M) and Cyber Security initiative skill (CS) were significant predictors of Computer Misuse Intention (CMI). User's awareness of computer monitoring and computer self efficacy were significant contributors to cyber security skill. While User awareness of security policy was a significant contributor to cyber security action skill. However, computer self-efficacy has no direct influence on misuse behavior.

In a study of 'Privacy, computer crime and IT misuse' among 516 Midwestern college students[29] found that more than a third of business students (undergraduate and graduate) had misused computer system resources in their lifetime. The study also revealed that students who had read computer misuse policy committed more abuse than others. In other words, those who know about computer security are the ones that often engage in cyber crime. It also showed that greater familiarity with

computer was also an indicator of greater levels of computer misuse and that undergraduate misuse was lower than graduate misuse.

Spellar, studied the relation between psychopathy, basic personality, antisocial behavior and computer crime in a sample of 235 participants through Amazon' Mechanical Turk (MTurK). The result demonstrated a strong support for the relationship between psychopathy as measured with the Elemental Psychopathy Assessment Short Form (EPA-SF), personality, antisocial behavior and computer crime. It also suggests that computer criminal behavior, like other forms of antisocial behavior correlates with violent and non violent behavior and psychopathy.

Hu *et al*.[30] studied the cross cultural anecdote of computer hacking behavior of Chinese and American students. They found that some factors are consistent while others were distinctly different across the two samples. The result showed that moral belief about computer hacking are the most consistent antidote against computer hacking intention among the Chinese and American samples. However, playing computer games (Team sport) significantly increases versus decreases the intention to engage in computer hacking in the Chinese college students but has no significant effect on the American sample. Based on the result, each sample supports distinct dimensions of both the Routine Activity and Self-Control theories of criminal behavior.

Hinduja[31] had found that students who are highly skilled at internet activities are more likely to be software pirates than students who demonstrate a lower skill.

Ubonavicuis, examined how novelty-seeking. Behavior relates to illegal internet download among a young population. The study was based on data obtained through national survey in Lithuania. The result indicates a significant relationship between novelty seeking, attitude towards piracy and the frequency of illegal downloading of movies.

Lavin, predicted that participants who were higher in internet usage and internet behavior would be high in sensation seeking. The result indicate that internet dependants tended to spend more time online, use E-mail, surf the web, use chat room, use MUD and visit cybersex sites more often than non dependents. However, dependants scored significantly lower on sensation seeking, thrill, adventure seeking and excitement seeking behaviour than nondependent internet users. They therefore concluded that dependents interact with the internet using a motivation scheme dissimilar to the physical thrill and excitement that typically characterize sensation seeking archetype.

In a study of self control, thrill seeking and crime, Burt and Simons[32] hypothesized that thrill seeking behavior and self control have independent influence on offending. In other word, that motivation to process crime matters. They used 770 African-Americans to test the hypothesis and the result supported the hypothesis and indicated also that the effects of self control are contingent on the levels of thrill seeking behavior.

Hypothesis: The following hypothesis would therefore guide this research:

- That adventurism will not predict cyber criminal behavior among Imo State university undergraduates
- That information technology self-efficacy will not predict cyber criminal behavior among the undergraduate
- That age will not predict criminal behavior among the undergraduates

MATERIALS AND METHODS

Participants 200 male undergraduates of Imo State University were selected using convenient sampling method from four Student Hostel alliances namely, Bishop's Court Hostel Alliance, Front Gate Hostel Alliance, Aladinma Hostel Alliance and Amawire Hostel Alliance. Their ages ranged from 18-30 with a mean age of 24.80 and standard deviation of 2.97. The 40% were classified as young while 60% are young adults. A total of 57% of the participants are males while 47% are females.

Instruments: Three instruments used in the study include the Cyber Crime scale which was developed by conducting an initial interview with the Superintendent Police Officer at the State Police Force Headquarters Owerri and the District Crime Officer of Egbu police station. The essence of the interview was to understand what behaviour have been observed, reported and persecuted as cyber crime so far, by the law enforcement agency in Owerri. Information gathered were combined with those obtained from literature and used to compose an initial 46-item cyber crime scale. It was constructed in 4-point Likert format and scored directly from "Very true of me", 4 points to "Very untrue of me" scored 1. Sample items on the scale include "Extorting money from someone online is a game of the intellect not a crime" "I do not mind using a friend's device to do transactions he may not be aware of".

The Information Technology Self Efficacy Scale (ITSE) was developed by picking items from literature and adding them to modify and revalidate Murphy's computer self-efficacy scale. It consists of 21-items which reflect variety of information technology related skill and knowledge. It was developed in a 5 point\Likert

format, ranging from "strongly agree," and scored 5, to "strongly disagree" scored 1. The items are coded directly. Sample items on the ITSE scale include: "I feel confident storing any new software correctly in a computer system from online source" and "I feel confident cracking different networks into a single modem".

Adventurism scale was developed by reading through literature and listing 32 items which were later filtered to produce an initial 17-item scale. It was developed in a 3-point Likert form and scored directly from "Very true of me, 3 points to Very untrue of me, 1 point. It was also given to experts for face validity assessment and recommendation. Sample items of the scale include: " I often try new things just for fun or thrill even if most people think it is a waste of time" , "I like the feelings that come with taking risk" and "I often do things based on how I feel at the moment without thinking about how they are done in the past".

Both, the Cyber Crime scale, Adventurism scale, Information Technology Self efficacy scale and Zukerman Sensation Seeking questionnaire were administered to 40 undergraduates from the Mbaonu Ojike hostel alliance for validity and reliability computations. Analysis of the responses produced a Chronbach alpha reliability index of 0.76 and a norm of 42.5 for the Cyber Crime scale and reliability index of 0.82 and a norm of 52.5 for information technology self efficacy. Moreover, only items that attained 0.46 inter correlation index were included in the final scale. The scores were also subjected to item analysis to determine their index of difficulty and discrimination levels. Only items that loaded 0.40 and 0.60 difficulty and discrimination levels, respectively were included in the final scale.

The adventurism scale was administered along with Zukerman Sensation Seeking scale to the same participants all together for concurrent validation. It was constructed in a 5 point Likert scale ranging from strongly agree = 5 to strongly disagree = 1. It consists of 19-items coded directly. Analysis of the responses provided a correlation index of 0.74 with the Zukerman scale and a norm of 61. Altogether, the last scale consists of 17 item coded directly.

Procedure: Specifically, four Student Hostel Alliances around Imo State Universitry Owerri, were selected using simple random sampling, namely: Bishop's Court Hostel Alliance, Front Gate Hostel Alliance, Aladinma Hostel Alliance and Amawire Hostel Alliance. In each of the hostel alliance, the researcher selected participants using convenience sampling technique. Therefore, the researcher was able to select participants for this study using simple random sampling and convenience sampling technique respectively. This was because the researchers needed participants who are available and willing to participate in the study.

The researchers introduced themselves to the participants, created rapport with them, by briefly informing them about the aim of the study and assuring them of the confidentiality of their responses. They distributed the questionnaires to the participants. The researcher gave each participant 25 minutes to complete the questionnaire after which they collected them for coding.

The 220 questionnaires were distributed, 10 were incorrectly filled, 9 were rejected, 1 was misplaced and 200 were coded and analyzed.

Design and statistics: The design used for this study is cross sectional design. This is because the researcher used one-time-only observation of all variable necessary for the study. Multiple Regression Statistics was used to analyze the data collected.

RESULTS

Table 1-3 are presented the results of the computations of the data obtained from the field investigation for the study.

The result of the multiple regression analysis shows that 0.38 or 38% of cyber crime is predicted by a combination of age, adventurism and Info Tech self-efficacy and this is also statistically significant $f(3, 195) = 39.880$, $p = 0.001$.

Hypothesis 1: Analysis of the result also indicates that hypothesis two which states that adventurism will not significantly predict cyber crime was rejected, $\beta = -19.54$, $t(195) = -7.58$, $p = 0.001$. The result therefore indicates that adventurism significantly predicts cyber crime. Table 1 above also shows that adventurous undergraduates scored higher ($M = 66.90$, $SD = 17.03$) than non adventurous undergraduates ($M = 44.05$, $SD = 19.17$) in cyber crime.

Hypothesis 2: The result of the study also showed that this hypothesis which states that Information technology self-efficacy will not predict cyber crime was rejected, $\beta = -12.826$, $t = (195) = -5.27$, $p = 0.001$.

Table 1: The descriptive statistics for adventurism, IT self-efficacy and age as predictors of cybercrime

Variables	N	Mean	SD
Adventurous	136	66.90	17.0325
Non Adventurous	66	44.05	19.1740
High IT Self-efficacy	118	67.16	16.7005
Low IT Self-efficacy	81	49.60	21.2572
Young	80	54.85	22.2512
Older	119	63.48	18.6242

Table 2: Model summary

Model	R	R^2	Adjusted R^2	SE of the estimate
1	0.671[a]	0.0384	0.016	13.40256

[a]Predictors: (Constant), InfoTech self-efficacy, Adventurism, Age

Table 3: Regression analysis for adventurism, InfoTech self-efficacy and age on cyber crimes

	Unstandardized coefficients		Standardized coefficients		
Models	B	SE	(Beta)	T (B)	Sig. (SE)
1 (Constant)	94.769	6.224	-	15.225	0.000
Adventurism	-19.543	2.579	-0.438	-7.578	0.000
Information technology self efficacy	-12.826	2.433	-0.307	-5.271	0.000
Age	5.459	2.387	0.131	2.287	0.023

[a]Dependent Variable: cyber Crime

This demonstrates that information technology self-efficacy significantly predicts cyber crime among the undergraduates. Table 1 also shows that undergraduates with higher InfoTech self-efficacy scored higher (M = 67.16, SD = 16.70) than those with low IT self-efficacy (M = 49.60, SD = 21.26) in cyber crime.

Hypothesis 3: The analysis demonstrates that age accounts for the positive variance on cyber crime, $\beta = 5.46$, $t(195) = 2.287$, $p = 0.023$, hence, hypothesis one is rejected. This demonstrates that age is a significant predictor of cybercrime. Table one also indicates that older under graduates scored higher (M = 63.48, SD = 18.62) than younger ones (M = 54.85, SD = 22.25) in cyber crime.

In all, the three independent variables in this study significantly predicted cyber crime with adventurism accounting for the greatest variance on cyber crime (-0.438), followed by information tehnology self efficacy (0.307) and age (0.131) in that order. The negative value for adventurism, however, showed when adventurism is increasing cyber crime will be on decrease. This finding also applies for InfoTech self-efficacy. When InfoTech self-efficacy increases cyber crime will be on the decrease.

DISCUSSION

The result of the study shows that adventurism significantly predicts cyber criminal behavior among Imo State university undergraduates. This result is apparently supported by the findings of Ubonavicuis, etc. who found that novelty seeking behavior relates to illegal download from the internet of young people. It is also in line with finding reported in Wikipedia that adventure is among causes of cyber crime. However, the predicated relationship between adventurism and cyber crime in this study is inverse. This suggests is that as adventurism increases cyber crime decreases. This indication is that since adventurism denotes more of novelty seeking exploratory behaviour, undergraduates who are experimenting to discover the intricate novel and more fantastic nature of the internet world may be too busy or uninterested in getting into cyber crime. Of course, getting into cyber crime requires expertise knowledge of the technicality of computer operation including functional techniques of cyber security software and being able to predict successful the possibility of striking without being caught which most of these students lack. The result of the study also indicates that information technology self-efficacy predicts cyber crime. This is apparently consistent with similar findings in literature. For instance, though skill differs from self-efficacy, Hinduja[31] found that students who are highly skilled at internet services are more likely to be software pirates than students who demonstrate low skills. Cronan *et al*.[29] findings also showed that greater familiarity with computer was an indicator of computer misuse. However, the predictive value of information technology self-efficacy to cyber crime in this study is also inverse, indicating that as information technology self-efficacy increases cyber crime decrease. This implication is that the greater the undergraduates InfoTech self-efficacy the more they become aware of the consequences of engaging in cyber crime, the possibility of being identified at last and apprehended in the long run, so, they desist from it.

The result of this study indicating that age predicts cyber crime is not peculiarly different from other findings in literature. While Cronan *et al*.[29] found that age is not a significant factor in, Gopal and Sanders[23] found that younger students were more likely than older ones to engage in computer crime (piracy). Moreover, Seale *et al*.[24] found that age is inversely related to the amount an individual pirate software while Cronan and Al-Rafee[25] found that age has a direct relationship with the age the individual may pirate a software. The implication of this finding is that the relationship between age and cybercrime still needs to be explored further in empirical research before a definite conclusion can be drawn.

Significance of the study: The result of the study indicate that both adventurism and information technology self-efficacy inversely predicate cyber crime. This suggests that in efforts to reduce or eliminate cyber crime parents and education authorities should inculcate and intensify ethical training and moral guidance to youths and students in their use and exploration with computer and internet services. The finding also demonstrates that greater attention on control and guidance should be placed on young adults than adolescent. Government and corporate institutions need to put forward strategies and policies to engage these youths in skill training and

capacity development prior to graduation to preclude excess engagement in computer and internet exploration as compensation for idleness. The findings may also find significance in employee's placement in organizations. In terms of employment, personnel manager should prefer placing employees with high adventurist tendencies and high information technology self-efficacy in sensitive internet based positions than otherwise. The reason being that as adventurism and information technology self-efficacy increase cyber crime tend to decrease. Perhaps, as experiences with the computer and the internet increase the individual becomes more aware of the consequence of engagement in cyber crime and begins to withdraw.

CONCLUSION

The study was designed to ascertain if adventurism, information technology self-efficacy and age could predict cyber crime among Imo State university undergraduates. The 200 participants were selected using convenient sampling techniques from four Students' Hostel Alliances. Cross sectional survey design was used to gather data while multiple regression analysis was used to analyze the data. Result indicates that the three independent variables significantly predicted cyber crime among the students, a result that has significance for both youth training potential work engagement.

REFERENCES

01. Shinder, D.L., 2002. Scene of the Cybercrime: Computer Forensic Handbook. Syngress Publishing Inc, Massachusetts, USA., Pages: 719.
02. Okeshola, F.B. and A.K. Adeta, 2013. The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. Am. Int. J. Contemp. Res., 3: 98-114.
03. Omodunbi, B.A., P.O. Odiase, O.M. Olaniyan and A.O. Esan, 2016. Cybercrime in Nigeria: Analysis, detection and prevention. FUOYE J. Eng. Technol., 1: 37-41.
04. Cluley, G., 2016. Citibank IT guy deliberately wiped routers, short down 90% of firm's network across America. DataBreaches LLC., USA.
05. Broadhurst, R., P. Grabosky, M. Alazab, B. Bouhours and S. Chon, 2014. An analysis of the nature of groups engaged in cyber crime. Anal. Nature Groups Engaged Cyber Crime Int. J. Cyber Criminology, 8: 1-20.
06. Bort, J., 2013. The American library association has given Aaron Swartz its first ever posthumous award. Inside Inc., London, UK.
07. Eimiller, L., 2011. Florida man arrested in operation hackerazzi for targeting celebrities with computer intrusion, wiretapping and identity theft. Federal Bureau of Investigation, Washington, USA.
08. Davies, C., 2010. Welcome to dark market-global one-stop shop for cybercrime and banking fraud. The Guardian, London, UK.
09. Glenny, M., 2011. DarkMarket: CyberThieves, CyberCops and You. Alfred A. Knopf, New York, USA., Pages: 296.
10. US Federal Bureau of Investigation, 2011. Malware click fraud kingpin arrested in Estonia. US Federal Bureau of Investigation, Washington, USA.
11. Constantin, L., 2012. Improved Carberp banking malware will target North American banks. IDG Communication, Framingham, Massachusetts.
12. US Atorney's Office, 2013. Eight members of New York cell of cyber crime organization indicted in $45 million cyber crime campaign. US Atorney's Office, Charleston, West Virginia.
13. Aspan, M. and K. Soh, 2011. Citi says 360000 accounts hacked in May cyber attack. Thomson Reuters Corporation, Toronto, Canada.
14. Italino, L., 2012. Ex-staffer sentenced to 2-6 years for hacking into Gucci's system. NYP Holdings, Inc., New York, USA.
15. The Guardian, 2013. LulzSec hacktivists handed long jail sentence for hacking. Guardian News & Media Limited, London, UK.
16. Chickowski, E., 2011. The most notorious cybercrooks of 2011-and how they got caught. Dark Reading, Informa PLC, London UK.
17. Liebowitz, M., 2012. UK hacker sentenced for stealing 8 million identities. NBC News, New York, USA.
18. US Departmenst of Justice, 2002. Warez leader sentenced to 46 months. US Department of Justice, Washington, USA.
19. Cohen, A., 2013. Was Aaron Swartz really killed by government. TIME USA, LLC., USA.
20. Cai, T., L. Du, Y. Xin and L.Y. Chang, 2018. Characteristics of cybercrimes: Evidence from Chinese judgment documents. Police Pract. Res., 19: 582-595.
21. The Free Dictionary, 2016. American Heritage Dictionary of English Language. 5th Edn., Houghton Mifflin Harcourt, Boston, Massachusetts, USA.,.
22. Leonard, L.N., T.P. Cronan and J. Kreie, 2014. What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance or individual characteristics?. Inf. Manage., 42: 143-158.
23. Gopal, R.D. and G.L. Sanders, 1997. Preventive and deterrent controls for software piracy. J. Manage. Inf. Syst., 13: 29-47.
24. Seale, D.A., M. Polakowski and S. Schneider, 1998. It's not really theft!: Personal and workplace ethics that enable software piracy. Behav. Inf. Technol., 17: 27-40.
25. Cronan, T.P. and S. Al-Rafee, 2008. Factors that influence the intention to pirate software and media. J. Bus. Ethics, 78: 527-545.

26. Ajzen, I. and M. Fishbein, 1980. Understanding Attitudes and Predicting Social Behavior. Prentice-Hall, Englewood Cliffs, New Jersey, ISBN-13: 978-0139364358, Pages: 278.
27. Ajzen, I., 1991. The theory of planned behavior. Organiz. Behav. Hum. Decis. Process., 50: 179-211.
28. Choi, M., Y. Levy and A. Hovav, 2013. The role of user computer self-efficacy, cybersecurity countermeasures awareness and cybersecurity skills influence on computer misuse. Proceedings of the 8th Pre-ICIS Workshop on Information Security and Privacy, December 14, 2013, AISeL, Milano, pp: 1-19.
29. Cronan, T.P., C.B. Foltz and T.W. Jones, 2006. Piracy, computer crime and IS misuse at the university. Commun. ACM., 49: 84-90.
30. Hu, Q., N.C. Vukadinovic and D.R. Lynam, 2017. Computer criminal behavior is related to psychopathology and other psychosocial behavior. Criminal Justice, 51: 67-73.
31. Hinduja, S., 2003. Trends and patterns among online software pirates. Ethics Inf. Technol., 5: 49-61.
32. Burt, C.H. and R.L. Simons, 2013. Self-control, thrill seeking and crime: Motivation matters. Criminal Justice Behav., 40: 1326-1348.