INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

FRAUD THEORIES AND GLOBAL CYBERCRIME DURING THE COVID-19 PANDEMIC: THE EXTENDED S.C.C.O.R.E MODEL

Joshua, Abimbola Abosede, Alao, Olubunmi, Ige, Oludele Emmanuel

Department of Accounting, Mountain Top University, Kilometre 12, Lagos-Ibadan Expressway, Prayer City, Ogun State, Nigeria

Department of Accounting, School of Management Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Department of Accounting, School of Management Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria.

Abstract

The study focused on the impact of present covid-19 cybercrime predicament on every facet of individual lives and organisations with the aim of elaborating the fraud theories. The paper review most widely and accepted fraud models so as to establish the motive behind why people commit fraud. Some of the fraud theories reviewed in the study include Anomie theory, Routine Activity theory, Fraud Triangle theory, Rational Choice theory, Fraud Diamond, Fraud Scale, M.I.C.E theory, the ABC of While-Collar Crime theory, Fraud Pentagon and Fraud Hexagon. The study found out the major factors causing fraudulent activities most especially in the pandemic include opportunity emanated due to the global economic crisis and thereby conclude in formulating another model S.C.C.O.R.E.E which is presented diagrammatically as the Fraud Heptagon. The study included an additional acronym E to the initial S.C.C.O.R.E which stands for the economy exploited both by individuals and firms to perpetrate fraudulent activities as a result of the pandemic which have devastating effects on the economies both in the developed and the developing countries. The study opined that the fraud theories should be updated in line with the current economic condition that birthed an outrageous rate of global cybercrime and thereby contributed to the field of theoretical development. Therefore, the paper contributes to the development of fraud theories by identifying the major motivating fraud factors which enabled the occurrence of fraud and stands as a reference point for future researches.

Keywords: Cybercrime, Covid-19, Fraud theories, Cybercriminals and Cyberterrorisms
JEL Classification: H12

Introduction

The COVID-19 pandemic is an unprecedented challenge in several ways for our lifetime as it has impacted both on individual lives, government and the global economy (Bruce, 2021). The global pandemic has posited pressure most especially financial and operational pressure both on corporate entities and individuals across the globe. The pressure has mounted higher level of financial risk which include loss of revenue, uncertainty in the going concern status of companies, drastic reduction in the market demand and trading, chronic liquidity problems and final winding up of some companies (Deloitte, 2020). However, emanated from the economic risk is the act of justifying fraud perpetrated by manipulating financial information, assets misappropriation, misrepresentation of financial and non-financial information and other fraud schemes (Nivette, Zahnow, Aguilar, Ahven, Amram, Ariel, Burbano, Atolfi, Baier, Bark, Beijer, Bergman, Breetzke, Concha-Eastman, Curtis-Ham, Davenport, Diaz, Fleitas, Gerell, Jang, Kaariainen, Lappi-Seppala, Lim, Revilla, Mazerolle, Mesko, Pereda, Peres, Poblete-Cazenave, Rose, Svensson, Trajtenberg, Lippe, Velldkamp, Perdomo and Eisner, 2021; Deloitte, 2020).

The World Health Organisation announced the pandemic on March 11th, 2020 as a global emergency issue which thereafter some measures were instilled to curtail the spread of the virus which include maintaining social distance, lockdowns, travel bans, closure of social and religious gathering as well as schools. These measures emphasised stay home for everybody except for essential activities which led to decline in physical movement to over 80% (Amy et al, 2021; Katelyn and Tammy, 2021). According to Financier (2021), the lasting effect of the pandemic is an issue of fraud which was in line with the report of the 'Fraud in the wake of COVID-19' written by the Association of Certified Fraud Examiners that over 80% of the anti-fraud experts surveyed reveal a significant increase in the overall level of fraud globally in 2020 and beyond (Bruce, 2021).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

The UK Research and Innovation (UKRI,2021) stressed the fact that the pandemic emanated new opportunity for fraud as fraudsters exploit the existence of the new vulnerabilities such as the systems, organisations, members of the populations through sophisticated cyber-enabled schemes. The global pandemic aggravated increase in the level of fraud commitment as well as its complexity. For instance, Action Fraud reported on the 7th of May, 2020 that about 1467 victims of COVID-19 cyber related crimes had lost an amount to the tune of £2,996,252 (UKRI, 2021). Bruce (2021), the President and the CEO of the Association of Certified Fraud Examiners (ACFE) pointed out that the global looming economic downturn has a number of long-lasting implications which include majorly an explosion of fraud.

The transition from physical working to remote working from home, shopping online, having virtual meetings and social events had changed individual patterns of living and responses from the government has impacted on the economies as well as the ecosystem of cyberworld (Hakak, Khan, Imran, Choo and Shoaib, 2020). As consumers feel convenient to transact online and as service providers enjoy massive online services, not all the online transaction can be seen legitimate as cybercriminals exploit different creative means of reaching the online service users thereby increasing the level of cybercrime victims, huge financial loss, disruption in services, institutional and individual anxiety (Hakak et al, 2020; Katelyn and Tammy, 2021). Adepegba (2020) expatiated the report of the Federal Bereau of Investigation (FBI) on how about 20 countries globally have lost more that $4.1 trillion to cyber attacks most especially during the covid-19 as the fraudsters targeted covid-19 aid relief and other palliatives to help small businesses and individuals which was a 69 percent increase over 2019 cyber cases.

The increased in online dependency of individual and corporates create new opportunities with individuals and businesses more vulnerable to cyber-attacks as the crime opportunities have shifted from the offline to online environment (Buil-Gil, Miro-Llinares, Moneya, Kemp and Diaz-Castano, 2020; Groenendaall and Helsloot, 2021; Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple and Bellekens, 2020). The COVID-19 pandemic has been significantly associated with a drastic change in crime opportunities as sudden rush to pandemic crisis causes significant cyber security gaps in organisation and employees were asked with immediate effect to remote working from home without considering the implications of cyber security on them, the ICT as well as the organisation at large (Collier, Horgan, Jones, and Shepherd, 2020; Groenendaall and Helsloot, 2021). Katelyn and Tammy (2021) stressed the psychological effect of COVID-19 as the cybercriminals take the advantage of the pandemic through the psychological vulnerabilities of their victims' anxiety, stress, anger, frustration and other emotional vulnerabilities.

In order to restore the confidence of consumers to pick up and trust e-commerce, countries of the world have established legal frameworks that can adequately protect the citizens online. The United Nations Conference on Trade and Development (UNCTAD) survey revealed that countries which include Brazil, Korea, New Zealand, South Africa and Thailand have drafted legislations on data protection and privacy. However, to protect online transaction of businesses and consumers is a matter of just legislation. It requires enforcement which some developing countries have insufficient capacity and resources to enforce (UNCTAD, 2020).

As of early September 2021, the COVID-19 cases have rose to almost 220 million cases globally with about 5 million death cases reported (WHO, 2021). However, the pandemic as foster effects such as the redistribution of wealth and welfare policies as well as the aggravated cybercriminals globally (Matthewman and Huppatz, 2020). In Nigeria as other part of the world, cybercrime is not primitive as the cybercriminals perpetrate the criminal act through the emails, text messages, websites and social medias. They usually demand for people's information so as to have access for their wilful intention (Eboibi, 2020). Several studies have been carried out to establish the effect of COVID-19 pandemic on individuals and businesses globally most especially on the issue of cybercrimes. However, the study aimed at unravelling the pandemic as a major cause of cybercrimes globally and thereby establish an extended model with the prevailing economic condition.

Literature Review

The global COVID-19 pandemic and cybercrime

The COVID-19 pandemic also led to global tsunami of cyber threats which was evidenced from the report of Interpol on the survey of 48 countries on the cybercrime effects of the pandemic in addition to economic and health crisis. Covid-19 is also refer to as the novel coronavirus, SARS-CoV-2 or 2019-nCoV is an emerging pandemic that has claim lives and introduce new normal to people, businesses, economic and every other

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

spheres of life worldwide. Countries of the world such as UK and US made legislation and regulations yet uncover the issue of cyber coronavirus crime globally. The cybercriminals exploit the opportunity created by the pandemic to perpetrate crime (Eboibi, 2020). COVID-19 pandemic is a remarkable phenomenon that altered every phase of lives and created what could be referred to as the new normal as individual, corporate entities and the societies at large were left in the vulnerable condition (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple & Bellekens, 2021).

Apart from impact on individual lives and businesses, the rate of cybercrime aggravated during the pandemic as the increase in the rate of anxiety emanated from the pandemic heightened the potential of cyber-attacks. Cybercriminals prey increasingly on the fear of people on COVID-19 virus as they offered fake cures for sale on the Internet and defrauding through the sale of non-existent hand-sanitizer, medical Personal Protective Equipment (PPE) and medicines or hygiene products. Other frauds include the offer of services such as unsound investment advice (including cryptocurrencies) and incorrect medical advice and diagnosis. One major online pornography site offered free subscription to users from one country, thus increasing the risks of malware downloads and sextortion (UNODC, 2020).

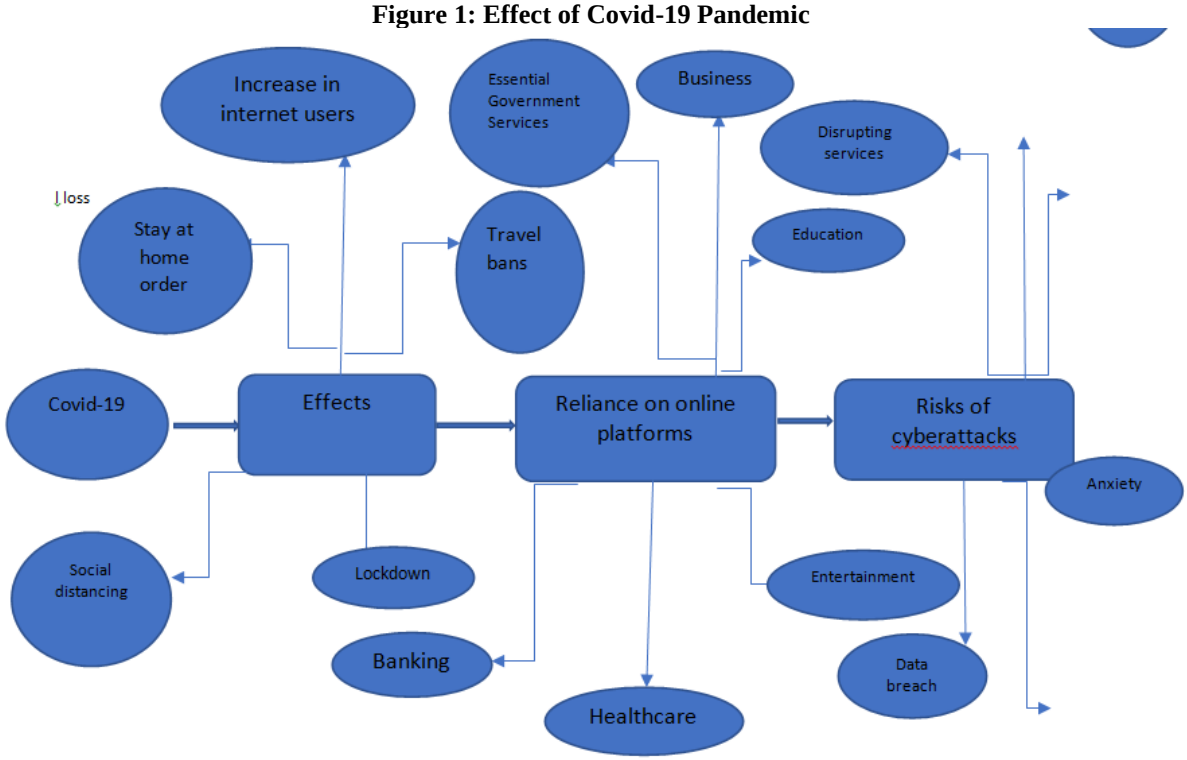
Before the advent of COVID-19, cybercrime was persistent and often transnational. According to Accenture, the cost of cybercrime cross-country increased within the period of 2017-2018 by 12% while the total global value at the risk of cybercrime may be as high as $5.2 trillion in the next five years (Hakmeh, Taylor, Peters, Ignatidou, 2021). However, with the emergence of covid-19, the rate of cybercrime has grown worse to a certain level. The report issued by Interpol revealed that between January 2020 to April 2020, about 907,000 spam emails, 48,000 malicious URLs detected and 737 incidents with malware were detected all related to covid-19 (Jochims, 2020). Cybercriminals tried modifying their mode of operations during the pandemic crisis as both private and public users of online remote are not spared from the attack. Companies migrate from physical work environment to virtual while schools also engaged in online classes, individual transacted online while religious activities have been shifted from physical gathering to online services which had led to the implementation of remote networks, applications and systems. However, cybercriminals seek conditions that will enhance their criminal activities and the pandemic crisis happens to be a profitable phenomenon since the emergence of cybercrime (Jochims, 2020).

Millions of dollars have been ransomed by the cybercriminals from businesses during the pandemic using cybercrime tactics such as social engineering, phishing and other hackers' tools. Over 80% of successful data breach ended up in defrauding people rather than exploiting flaws in computer code as over 60% of the data breach involves schemes engaged to swipe people's login details for instance, the phishing schemes (Patterson, 2021). Cybercriminals are serial entrepreneurs who depend solely on the lapses of peoples' judgement as people has less concern to develop cybersecurity during the pandemic when shift to remote way of doing things (Mahadevan, 2020). There has been speculation that as way of life was shifted to remote during the crisis, there will be an existence of cybercrime as a tsunami targeting the insecure personal wifi networks and computers (Sullivan, 2020).

Cybercriminals take the opportunity of the latest trend emanated from the pandemic events to spam potentials victims with phishing emails which are the mails sent to assume fake identity by the sender and pretending to offer something that the recipient may need or want in order to trick the recipient into diverging confidential information (Fruhlinger, 2020). Phishing emails are customised to fit the local contexts as global opportunity exist for phishing attacks. Japan was the first country with the use of COVID-19 such as phishing where Trojan was used to fooled the computer users in downloading it as a legitimate software with the intention of harvesting users' financial information and credentials (Okereke, 2020). Countries such as Canada and Switzerland detected malware through websites disguised to be official offering advises to people on the treatment and prevention of COVID-19 which looks believable (Coopers, 2020). As the virus spread so is the increased in the scale of cybercrime. In USA, reports have mentioned that phishing messages seems originated from the Centre for Disease Control (CDC) which solicited donations for COVID-19 vaccine development (Mahadevan, 2020).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Figure 1: Effect of Covid-19 Pandemic



Overview of Cybercrime Activities

Phishing

Phishing is a high-level identity theft that deprive people of their personal information and identity as well as defrauding business most especially the financial institution (Rodger, 2008). Phishing is a perverse act as it aimed at attacking the information system in order to gain access to personal and official information useful to exact gains for the perpetrators through identity theft (Wada and Odulaja, 2012). The focus of phishing act is to pose significant dangers for unsuspecting victims as it remains one of the swiftest global threats on the cyberspace. There is a need for technology innovation collaboration between various stakeholders to combat phishing activities. Phishing activities involves the presentation of highly impressive and credible web-presence convincing enough to make victims forget the security measures installed in the web browsers (Rachna, Tygar, and Hearst, 2006). Millions of users lose billions of dollars in 2003 as result of providing information to unknown websites (Brush, Rosencrance and Cobb, 2020; Litan, 2004). In Nigeria, phishing activities involves preying on customers using Interswitch which is the organisation having the largest number of customers with electronic transactions (Wada and Odulaja, 2012). According the report issued by the Federal Bereau of Investigation (FBI) in 2020 about 20 countries of the world which include Nigeria, Mexico, Germany, Canada, United Kingdom, US, South Africa, Australia, Greece, France, Belgium, Mexico, India and other Nine countries lost over $4.1 billion to cyber scam (Adepegba, 2020).

Cyber terrorism:

Cyber terrorism is a consequence of widespread of unpredictable computer network attack which had caused severe economic disruption, civilian deaths, fear and qualifies to be termed terrorism (Denning, 1999). Cyber terrorism is an unlawful act perpetrated to coerce individuals, businesses and government to be involved in a political objective which can lead to a severe economic damage. In Nigeria, the 3rd quarter of 2020 revealed the massive effect of cyber fraud on the economic at large, the report from the Nigerian Communications Commission (NCC) indicated that the rate of internet subscribers as at April 2020, increased with over 2.5 million subscribers which is as a result of increase in the online activities of companies such as Jumia, Google and big tech giant to mention but a few (Emmanuel, 2021). However, emanated from an outrageous increase in the online transaction during the pandemic is the increase in the fraudulent activities reported by the Nigerian Inter-bank Settlement System (NIBSS) as the fraudsters succeeded 91% of fraudulent attempts (Emmanuel, 2021).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Cyber terrorism is an approach that is politically backed up with the intention of attacking information, computer systems, data and computer programs resulting in violence against the non-combatant targets (Search Security, 2009). Cyber terrorism is an act design to cause an extreme financial loss or harm (Wada and Odulaja, 2012). The terrorist attacks majorly banks, power plants, water systems, military installations and air traffic control centres. The cyber terrorists also exploit the cyber infrastructure to launder money so the purpose of financing physical terrorism (Tudor, 2001). Cyber terrorism could also be described as a malicious act of using computer system to disrupt the normal operations of critical infrastructures in the country (Lewis, 2002). Cyber terrorism could be depicted as cyber extortion whereby the hackers attack e-mail servers, website, computer system leveraging on ransomware in which victims are denied of services and yet demanding to pay ransome (Hassan, Lass and Makinde, 2012).

Cyber Stalking

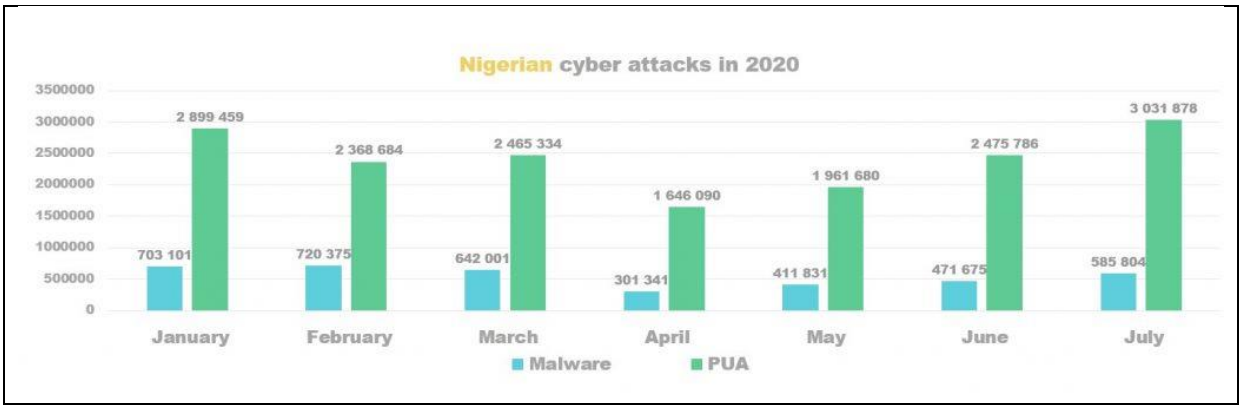
Cyber stalking is an act of online harassing of people repeatedly. Devices such as e-mails, internet and other telephone devices are used to stalk people (Ellison and Akdeniz, 1998). The cyber stalker follows the victims' online activities to obtain information and use such information for online verbal threatening. The cyber stalker use websites, social media, search engine to instil fear in their victims thereby concerned about their safety. The method is carried out deliberately, intentionally and methodically. It is an extension of physically engaged in stalking as it remains more common than that of physical stalking and the cyber stalker operate through the use of a high tech means to attack the victims (Wada and Odulaja, 2012). Cyberstalking usually can occasionally cause actual stalking and lead to a physical and emotional harm despite appeared harmless to people. Cyberstalking is a common phenomenon in racism and in expressions of hatred. The availability of website space and free emails has increase cyberstalking as a form of harassment as the content is most time inappropriate and even disturbing which leave the target audience anxious, distressed, fearful and worried which is an expression of cyberbullying (Gordon, 2021). The problems emanated from the cyberstalking is unquantifiable as some target audience might experience suicidal ideation and post-traumatic stress disorder. Therefore, cyberstalk is a phenomenon with a tendency of growing in complexity and scope.

Electronic Spam Emails

This comes in form of multiple emails sent to large number of people which can be in form of political, religious or commercial emails. The perpetrators adopt several means of reaching their target some which include the e-mail, the search engine, the blog, text messages with the emails spam as the most widely used. Spamming is common as no operating cost is involved and it is quite difficult to identify those perpetrating the act (longe and Chiemeke, 2008). The scammers take advantage of the pandemic by pretending that the disseminated messages are real. The scammers posed as real health organisationsa such as the World Health Organisation, Nigerian Centre for Disease Control to offer health counsels, health prevention and cure during the pandemic, tests and other covid-19 health related information. There are scammers websites offering fake covid-19 products such as the hand sanitizer, face masks, disinfectant wipes with the product never come on board. A good example of scamming activities in Nigeria is 419 mails or an advanced fee fraud in which victims have lost over $133 million to romance scammers (FBI,2021). Globally the top ten scamming countries especially during the covid-19 include Nigeria, India, China, Brazil, Pakistan, Indonesia, Venezuela, Pakistan, Phillippines and Romania (Chowdury, 2021). In 2020, Nigerian experienced over 20 million on malware attacks and potentially unwanted applications (PUA). However, when compared the cyber attacks in Nigeria with that of other African countries, cyber-attacks in countries like Kenya and South Africa is more severe (Onaleye, 2020).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Figure 2: Level of cybercrime in Nigeria in the year 2020



Adapted: Onaleye, (2020)

Consequences of Cybercrime in Nigeria and Beyond during the Covid-19 Pandemic

Cybercrime and Nigeria Economy

Cybercrime has affected the Nigerian economy even before the pandemic period as advancement in the technological level enhance diverse opportunities. The country's image has been negatively impacted since a single cyber-attack has an enormous and high multiplier implication on the economy as emanated from the act are consequences such as huge financial losses, theft of personal and intellectual property (Nabiebu and Akpanke, 2021). Over a million people fall victim of cyber attacks every year and the society are estimated to lose billions of dollars annually. According to Deloitte (2017), the federal government of Nigeria estimated the 0.08% of the country's GDP which is to the tune of N127 billion as the cost of cybercrime. In Nigeria, the estimated financial loss as a result cybercrime keep on rising as it stood at the tune of $649 million (N250 billion) in 2017 while in 2018 it was $800 million (N288 billion) and in 2019 hundreds of billion was lost due to cyber-crime (Guardian, 2019; Proshare 2020). Globally, cybercrime has cost the countries of the world about $500 billion annually and as at 31st December, 2020 global losses emanated from cybercrime is over $1 trillion which has dragged down the economy of the world drastically (Aliogo, 2021; Nigerian Communication Commission, 2016). The issue of cybercrime had seized the confidence of the populace as fear overwhelmed the potential investors and tourists.

Cybercrime and Nigerian Banking System

Opportunities abound for Banking system as a result of advancement in the use of technology which has also led to the risk exposure to the financial institutions at large. According to the Nigerian Deposit Insurance Corporation (NDIC), banks in Nigeria had lost more than N5 billion to the cybercriminals within the first 9 Months in the year 2020 as declared by the NDIC executive director (Onozure, 2021). When compare this situation to the previous years, the fraud cases in 2017 was to the tune of N12 billion and that of 2018 was about N40 billion. However, in 2019 it went up to over N200 billion as the fraud incidences could be connected to increase in cybercrime activities. This kind of criminal activities can cause an unrepairable damage to the growth of banking system both in Nigeria and beyond. The losses emanated from the cyberattacks not only affect banks individually but poses damaging risk to the financial system as a whole which has a serious implication on the economic growth and development both in Nigeria and globally. The increase in the use of online banking and transaction has created a very good platform for the perpetrators of cyberattack. Cybercriminals may fraudulently apply for loan online and funds can be embezzled using account takeover or wire transfer as well as disrupting e-commerce by denying online services (Wada and Odulaja, 2012). Online banking is also affected by the identity fraud which cast a significant fear on financial institutions' operations.

Cybercrime and Nigeria Oil and Gas Sector

Central to the fortune of economy in West Africa is the oil and gas sector. In Nigeria, the oil and gas sector contribute to more than 10% of the GDP and the revenue derived from petroleum export contribute to almost 90% of revenue from export and there is a compound annual growth rate of more than 10% in the crude oil production between 2020-2025. Surprisingly, in the east coast of US, cybercriminals have successfully slowing down the supply of petrol and diesel to the tune of 50%. Recently, ExxonMobil blocked over 200 million access

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

attempts to emails and internet on monthly basis. A single successful attempt of cyberattack on this crucial sector is enormous on the economy (Adewumi, 2021). There is a need for organisations, industries and government to critical look and address the issue of cybercrime.

Theoretical Review

Fraud theories and Covid-19 related Cybercrime

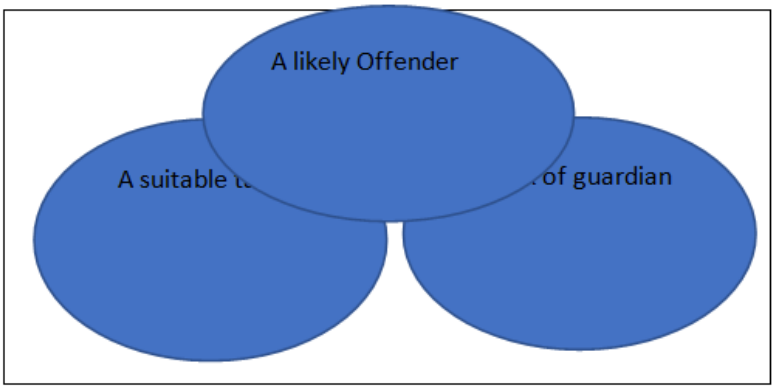
Anomie theory and cybercrime during the covid-19 pandemic

According to the propounder of the theory Emile Durkheim (1893), anomie is a state of breakdown in the system of a society to regulate the natural drives of people in a situation of societal changes as in the case of covid-19 (Cote, 2002; Ma & Mckinnon, 2020). The anomie theory opined that a rapid social change in an organic society will cause a state of anomie in the society. The theory explains the basis of why some society might have higher crime rates than the other society. A society with inadequate order and regulations will be vulnerable to criminal attacks. In a society with rapid social changes, anomie might lead to confusion, anxiety, fear, frustration and thereby provide a viable opportunity for cybercriminals to perpetrate their criminal act and thereby abuse the populace. Covid-19 provided a condition of new normal which emanated a drastic in the ways and manner people carried out their day-to-day activities such as remote working, travel bans, social distancing, virtual meetings and lectures, online shopping and transactions which poses challenges on cyber security. The theory provided vivid explanation as to the reasons why and how the populace became cyber fraud victims during the pandemic both from the perpetrator and the victimization perspective (Ma and Mckinnon, 2020).

Routine Activity Theory and Cybercrime

The theory was propounded by the Cohen and Felson (1979) who predicted that changes in situations or in the routine activities of people with lack of guardianship will enhanced the motivation of perpetrators to commit crime against the suitable targets. Routine Activity Theory (RAT) rely solely on changes in the current people's routine activities to online so as to explain clearly the issue of cybercrime most especially during the pandemic. Currently, people still work from home connecting virtually to their working place or businesses, the motivated offenders who seize every available opportunity on the online users that is the suitable targets. The theory asserts that the motivated offenders constantly focus on the attitudes, activities, and the current situation convenient to prey on the targeted victims. RAT affirmed that changes in the routine activities of people, organisation and social activities poses changes or trends in criminal activity which significantly impacted on individual and organisations' cyber defence. The covid-19 pandemic created a huge opportunity for cybercriminals to perpetrate their criminal activities by exploiting the widespread information on covid-19 infections, prevention and treatment (Govender, Watson and Amra, 2021). The motivated offenders send scam information like trojans, spyware and malware on covid-19 websites as well as widespread spam emails thereby tricking the online users to click on links that will enable the cyber criminals to have access to private information on computers and other mobile devices (Interpol, 2020). According to the report of PWC (2020), covid-19 brought up new opportunities for cyber threat actors to perpetrate and thereby gave recommendations to redress the cyber risks. RAT could be seen as a situational crime theory where the perpetrator seizes a criminal-friendly circumstances to commit crime as a result of an available opportunity (Govender et al, 2021).

Figure 3: Routine Activity Theory



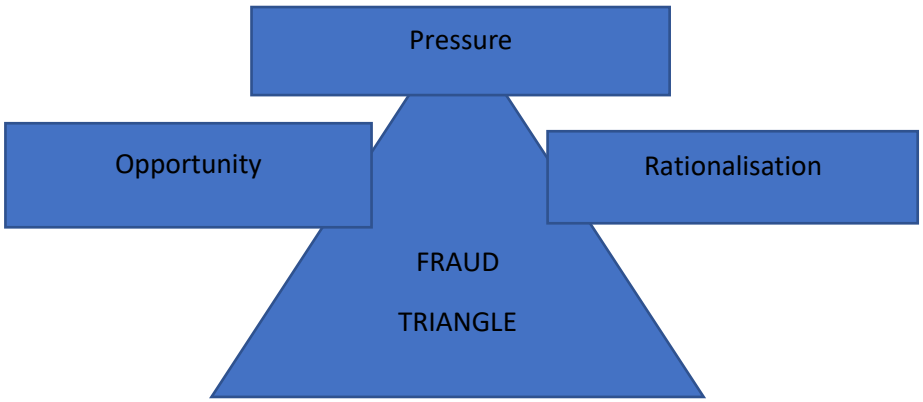
Adapted from: (Govender et al, 2021).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Fraud triangle theory and covid-19 pandemic

Fraud triangle model explains the motive for perpetrating fraud which consist of three elements indicated by Cressey (1953) which include pressure, opportunity and rationalisation (Abdullah and Mansor, 2015; Deloitte, 2020). In 2020, the global unemployment due to the COVID-19 pandemic increased by 33 million loss jobs with an increased rate of 6.5% (ILO, 2021). The present predicament has mounted pressure on organisations and individual to engage in manipulating financial statements while some still need to be alert to the pressures emanated from the effect of the pandemic that could lead to manipulate financial statement both at the level of corporate and operating level. Covid-19 effects could increase fraud perpetrated by the employees such as misappropriation of assets, embezzlement of funds, maximization of bonus scheme etc. (Deloitte, 2020). Organisations faced financially difficulty especially during the pandemic as a result of the lockdown which could rationalise fraud actions by the management as well as the employees as both feels the situation is not their fault. The massive increase in the online activities created opportunity for cybercrime. The chronic condition of the pandemic has led to huge cases of corporate bankruptcies and in fear of losing reputation and businesses some organisations will attempt juggling the fence by hiding their assets, diverting funds, presenting fictitious figures in the financial statement, trying to increase credit lines and many other measures. The profit motive during this period has provided motivational dynamism for theft actions, greediness, fraudulent activities while the white-collar organisations tend to disregard regulations controls for enhanced monetary gains (Ikechi and Nwadiubu, 2020). Therefore, the pandemic period enabled the justification of any unethical behaviour emanated therefrom due to the physical, emotional, mental and financial difficulties.

Figure 4: Fraud Triangle



Adapted: Cressey (1953) cited in (Ikechi and Nwadiubu, 2020)

The Rational Choice Theory (RCT)

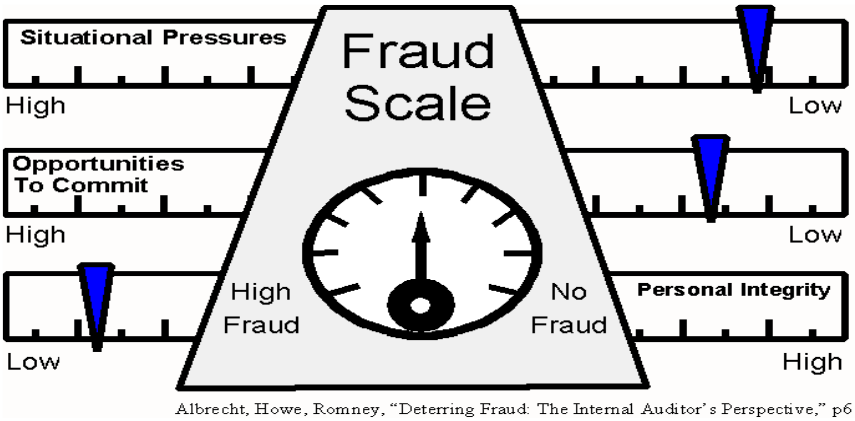
The RCM was an explanation of Cronish and Clarke (2014) adapted from economics that opined that crime behaviour is purposive in nature. The rationale behind the RCT is that the perpetrator act when balance the cost of the fraud with the benefits to be derived therefrom (Junger, Wang, & Schlomers, 2020). The criminals weigh their actions with the benefit emanated from such criminal acts by considering the end from the means and thereby take a drastic decision since envisaged benefits to be derived from the action. According to the RCT, offenders are rational in decision making but constraints due to the criminal ability and the available information relevant for the criminal act. Cornish and Clarke (2017) supported RCM as an act related to cybercrime that reveals an association between efforts put into the action and the reward obtained from the action, the more the efforts, the more the expected reward. The individual goals or wants determine what motivated them to act in which the action usually take place base on the information obtained about the circumstances to perpetrate the fraudulent activities. It might not be possible to achieve all the individual's goals at a particular point in time but the most important is the means to achieve the goals. Therefore, rational individual chooses a course of action which is best suited and can guarantee the highest level of satisfaction.

Fraud Scale

Fraud scale theory was propounded by Albrecht, Howe and Romney (1984). The elements of fraud scale are modifications of fraud triangle which include situational pressure, personal integrity and perceived opportunity (Ikechi and Nwadiubu, 2020). The theory opined that in a situation where perceived opportunities and situational pressures are high, there is high tendency of committing occupational fraud. Albrecht stated that

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

when ethics, responsibilities and honesty is being violated, there is tendency that accounting fraud will take place (Puspasari, 2016). Rationalisation occur as a result of ethical problems



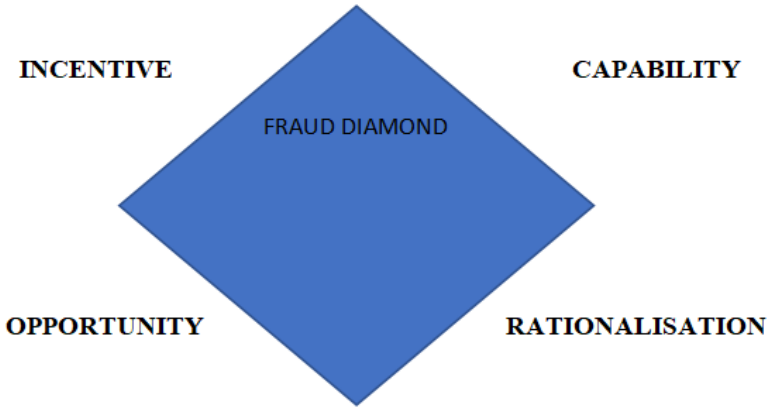
Albrecht, Howe, Romney, "Deterring Fraud: The Internal Auditor's Perspective," p6

Fraud Diamond Theory

The Fraud Diamond Theory was an extension of Fraud Triangle has argued by Wolfe and Hermanson (2004) with the addition of the fourth element referred to as capability. The capability can be ability of the fraudster to identify fraud opportunity either as a result of the position occupied or as a result of the adequate knowledge obtained. The propounders opined that fraud can only take place if the perpetrator has the capability or the skills to commit fraud regardless of the opportunity and the perceived pressure (Abdullahi, Mansor and Nuhu, 2015; Puspasari, 2016). However, while opportunity is the door way to perpetrate fraud, rationalisation is the legal ground for committing it. All the elements are so interrelated that they must all present before the fraud can be committed while pressure can make someone seek the opportunity of perpetrating fraud, opportunity can be backed up with rationalisation. However, despite the presence of the three aforementioned factors, until the fraudster has the ability to do so, there is high tendency that fraud might not take place. However, opportunity created by the pandemic has led to cybercrime creating threat for individuals and businesses.

Puspasari (2016) opined that the elements in the Fraud Diamond could be termed observable or non-observable. It is observable when outside parties such as the auditors and other employees could observe and get information from the fraudsters and however non-observable when information cannot be obtained about the elements of fraud from the perpetrators. Elements such as capability and opportunity can be observed by the auditors since the opportunity can be associated with weak internal control system while pressure can either be observable or non-observable. Finally, rationalisation is non-observable because it is not possible to read the mind of perpetrators

Figure 5: The Fraud Diamond



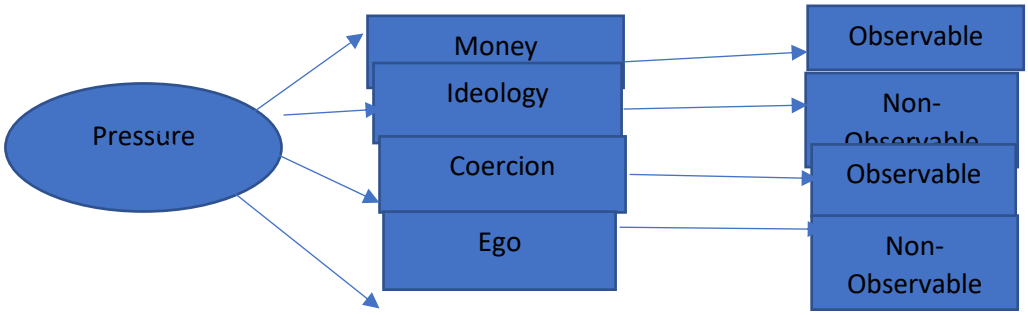
Adapted: Wolfe & Hermanson (2004) cited in Abdullahi et al (2015).

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

M.I.C.E Theory

The acronym of M.I.C.E stands for Money, Ideology, Coercion and Ego and according to M.I.C.E theory, these are the four factors that motivate the occurrence of fraud (Kranacher, Riley and Wells, 2010). These four factors can be regarded as being observable and non-observable. For instance, auditors can easily observe money through the financial needs of firms or individual and can also determine coercion existing in a particular work environment but there will be difficulty in determine the intention of individual as a result of ideology and ego (Puspasari, 2016). The theory focused on expanding the fraud triangle by extending the perpetrators scope of committing fraud by emphasising on fraudsters' behaviour (Ardi, Sulistyo and Roziq 2019). When a financial pressure exists, issues such as urgent taste of life style, family needs and debt will be obvious. MICE theory stressed on perpetrators behaviour of seeing fraud as a benefit and that illegal means of getting his money will not be harmful because the money can still be giving for charity donations. Coercive element is an indication that a third party threatening or forcing others to commit fraud for instance a manager forcing the subordinate to manipulate figures so as to embezzle fund (Ardi et al, 2019). Ego could be depicted as a desire to maintain or obtain a better taste of lifestyle so the fraudster feels no act of being apprehensive. M.I.C.E model can be diagrammatically presented as stated below:

Figure 6: The M.I.C.E Theory



Adapted: Puspasari, (2016**)**

The ABC of White-Collar Crime

The ABC theory tries to clarifies the scope of fraud triangle as regards the activities of fraudsters in which the behaviour of the perpetrators of fraud is the major root of perpetrating fraud through both the psychological and sociological means (Ramamoorti, 2008). According to the theory, A refers to as the bad apple which means the fraud carried out personally by an individual. The B refers to the bad bushel meaning that the fraud perpetrated collectively while the C refers to bad crop meaning fraud perpetrated collectively with the influence of a larger cultural and social background. The bad crop is most dangerous among the three in which the fraudulent behaviour of leaders in the organisations or in the society at large influence the younger generation and later become a culture in the entire organisation (Ardi, Sulistyo, and Roziq, 2019; Massiljev and Alver, 2016; Puspasari, 2016).

The S.C.O.R.E Model and the S.C.C.O.R.E Model

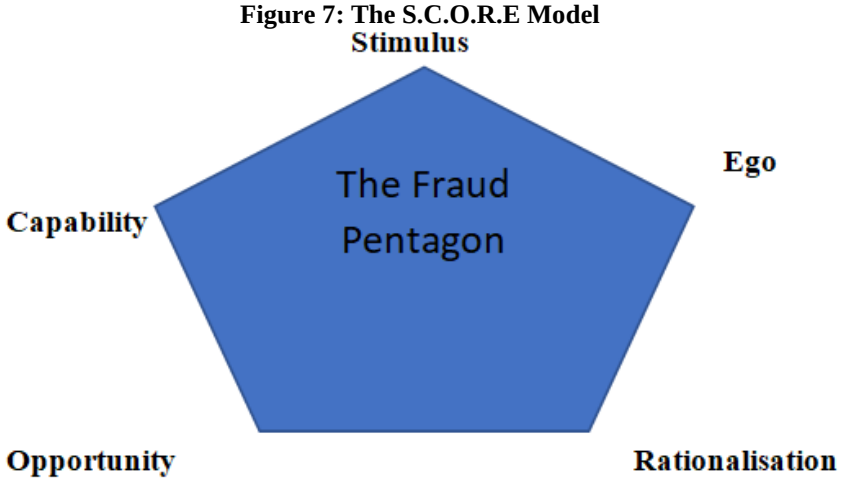
The SCORE Model

The SCORE model is an acronym that stand for stimulus, capability, opportunity, rationalization and ego (Vousinas, 2019). The theory is an extension of both fraud triangle and fraud diamond. The elements of S.C.O.R.E model are factors that motivate people to engage in fraud activities as they are the major determinants for the occurrence of fraud. Stimulus or incentive is of both financial and non-financial in nature which is the pressure for committing fraud. The pressure can be as a result of the need to meet up with a target demand most especially during the period of crisis like the prevailing COVID-19 pandemic. Capability is the ability to carry out the fraudulent act as many frauds occur due to the capability of the person carrying out the act having the right person with the right ability to perpetrate the fraud. Opportunity is the gateway to commit fraud while the stimulus and rationalisation motivated the entrance of fraudster into the door opened by opportunity as the perpetrator believed that he can act without being noticed. Opportunity can be created as a result of position occupied by individual within an organisation which can be perceived as real and not implicit. Finally, rationalisation is an act of justifying fraudulent activities as fraudsters can see themselves being honest and not as criminals (Vousinas, 2019). According to Kranacher et al (2010), ego is a major factor of why people

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

commit fraud and it is common in the history of white-collar crime which is the bedrock for committing largest frauds and notorious frauds at all time. All the elements of S.C.O.R.E model must present before fraud can actually take place.

Figure 7: The S.C.O.R.E Model

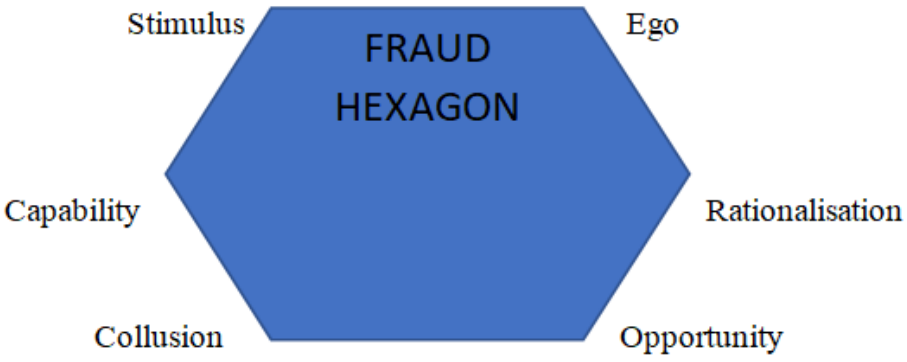


Adapted: Vousinas, (2019).

The S.C.C.O.R.E Model

In addition to the S.C.O.R.E model, an element of collusion was found as another factor responsible to fraudulent activities. The term collusion could be referred to as a deceitful act or agreement between two or more parties to defraud the third party of his privileges, employees in an organisation or from multiple organisations or jurisdictions. Collusion is a growing issue that is seemed not easy to stop as fraudsters prefer their own people to be in strategic places and many innocent people can be coerced into it due to dishonest culture and fraudulent environment. Many frauds committed in an organisation are mostly from the higher authorities threatening the subordinates to perpetrate the fraudulent act. Collusion can be voluntary as fraudsters exploit their power obtained through the position occupied in the organisation to take the advantage of others. ACFE reports on occupational fraud and abuse (2016) also revealed the significance of collusion as a larger part of fraud committed emanated from people' collusion to commit fraud. Therefore, collusion forms the sixth elements that extend the S.C.O.R.E model to S.C.C.O.R.E model which can be applied in white collar-crimes and the becoming fraud hexagon as presented below:

Figure 8: The S.C.C.O.R.E Model



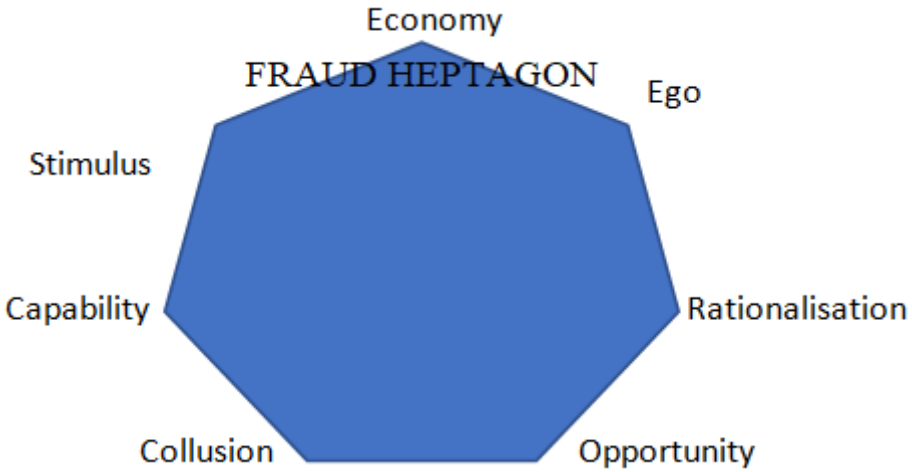
Adapted: Vousinas, (2019)

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

The S.C.C.O.R.E.E Model and the cybercrime

The impacts of the pandemic on the society and the economy at large cannot be overemphasised which influence and encouraged organised crime and illicit markets (UNODC, 2020). The enforcement of social distancing, travel bans and all forms of isolation which reduced both the production and the supply of commodities drastically to meet the enormous demand and internet facilities became a new normal (Kemp, Buil-Gil, Moneva, Miro-Llinares & Diaz-Castano, 2021). However, fraudsters have strategized themselves to take the best of the opportunity due to the pandemic. According to Interpol (2020), there has been a sharp increase in the rate of cybercrime activities as a result of the pandemic both against businesses and individuals. The increase in the cybercrime rate is expected has many business and people migrate from physical way of new things to the new normal of virtual as daily activities changed due to the COVID-19 pandemic. The vulnerability of the pandemic has enabled the criminals to exploit the opportunity for cyber terrorism and vulnerable people are being exploited by the criminals who use strategies such as phishing, online scams (Europol, 2020). The pandemic has hit every corner globally in which lives and societies have been reinvented. The Interpol recorded that criminals are taking the advantage of increase in the level of security vulnerabilities as a result of remote working to steal information both from individual and corporations and thereby causing disruptions. In the crisis period like the covid-19 pandemic, the fraudulent act potentials grow outrageously due to the recession in the economy and pressure therefrom posed on the populace most especially businesses to meet up with set target and to preserve reputation. Therefore, the fraud heptagon came up as a result of fraudulent activities due to the economic pressure prevailing globally beyond human emanated from the pandemic.

Figure 9: Fraud Heptagon



Source: Author's design

Conclusions and Recommendations

Fraud is dynamic, complex and adapts to changes in the prevailing environment which grows most especially during the period of financial crises and economic distresses. It is diverse in nature with diverse definitions and models to explain the motive for committing fraud. The issue of cybercrime is a global phenomenon that became outrageously rampant during the period of covid-19 pandemic. The models highlighted above and many others not mentioned in the study are evidences that no single model of fraud fits for all situation. Due to the pandemic, this study updated the existing fraud models to adapt to the economic condition arose as a result of the current development. The incidence of cybercrime is a crucial lesson to developing and developed countries of the world as cybercrime impede the development of the economy in the developing countries and also hampered the financial system globally. The internet penetration in the developing countries including Nigeria has gone beyond the threshold of 15% which gave opportunity for more malicious activities. However, digitalisation is the only means by which global full potentials and the UN Sustainability Development Goals (SDGs) could be achieved but the cyberthreat experienced in the developing countries due to the security problems has been endangering the economic enhancement since the high cost of security infrastructures are not affordable. The developed countries are not exempted from this predicament as cybercriminals targeted and

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

exploit the digital infrastructures of this countries to carry out their illicit act. The countries of the world need to act fast and effectively against the huddles of cybercrime as the effects of cybersecurity issues has significant implications not only in the developing countries but also to the global world. It is worthy of note the emphasise the cybercrime is flourishing due to technology related issues in the developing countries which can be addressed and reduced instituting governance intervention that could enforce security standards in the major sectors of the economy. There could be security dialogue between the government and vendors for the provision of more security enhanced products and services.

The high incidence of cybercrime could be traced to human related factors such as unemployment, low wages and high rate of poverty most especially in the developing countries mostly in Nigeria. A government intervention measure such as education by culcating the aspect of cybersecurity into the school curriculum for more awareness and as a measure to address the issue of cybercrime. There should be national and global cybersecurity strategies to enhance a long-term general governance framework. The impact of cybercrime on the economies of both the developing and developed countries could be devastating which include reduction in the investment rates, increased in the regulatory litigation and fines for business and also hampering of economic development which can negatively affect the economic inclusion of the poor. The developing and developed countries need to ensure that ICT is strengthened with the aim of being cost effective and efficient. Therefore, the author built on the existing theories such as the fraud triangle, fraud diamond, fraud pentagon and fraud hexagon which is the same as the S.C.C.O.R.E model with the acronym (Stimulus, Capability, Collusion, Opportunity, Rationalisation and Ego to create a new model fraud heptagon (S.C.C.O.R.E.E – Stimulus, Capability, Collusion, Opportunity, Rationalisation, Ego and Economy) as a result of the enormous increase in the rate of global cybercrime emanated from the global economic issues that mounted pressures on every facet of lives both on individuals and corporate entities with the focus of meeting targets. This study aimed at contributing to the literatures on the development of fraud theories by critically evaluating factors that motivated fraudulent activities and thereby developed model that will serve as reference for future studies on the subject matter.

References

1. Adepegba, A. (2020). How Nigeria, US and other 19 countries lost $4.1 trillion to cyber fraud in 2020 – FBI. https://punchng.com/how-nigeria-us-19-others-lost-over-4-1b-to-cyber-fraud-business-scam-in-2020-fbi/
2. Adewumi, T. (2021). Cybercrime is an existential threat to economic growth of West Africa. https://guardian.ng/ama-press-releases/cybercrime-is-an-existential-threat-to-west-africas-economic-growth/
3. Aliogo, U. (2021). West Africa: Nigeria lost N5.5 trillion to cybercrime in 10 years. https://allafrica.com/stories/202104260948.html
4. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23:sup1 S47–S59. https://doi.org/10.1080/14616696.2020.1804973
5. Bruce, D. (2021). Coronavirus pandemic is a perfect storm for fraud. https://www.acfe.com/press-release.aspx?id=4295010491
6. Brush, K., Rosencrance, L & Cobb, M. (2020). Cybercrime. https://searchsecurity.techtarget.com/definition/cybercrime
7. Collier, B., Horgan, S., Jones, R. and Shepherd, L. (2020). The Implications of the COVID-19 Pandemic for Cybercrime Policing in Scotland: A Rapid Review of the Evidence and Future Considerations, Edinburgh: The Scottish Institute for Policing Research, Research Evidence in Policing.
8. Cornish DB and Clarke RV. (2014) The reasoning criminal: Rational choice perspectives on offending: Transaction Publishers.
9. Cornish, D. B., & Clarke, R. V. (2017). The reasoning criminal: Rational choice perspectives on offending. Environmental criminology and crime analysis (pp.29–61). Taylor & Francis Group: Abingdon.
10. Cooper, S. (2020). Canada's cyber agency dismantling fake government coronavirus pandemic response websites, Global News, 13 March 2020, https://globalnews.ca/news/6673497/canada-csec-fakecoronavirus-pandemic response-websites/; Bluewin,Kriminelle nutzen Corona-Krise, 14 March 2020, https://www.bluewin.ch/de/news/vermischtes/kriminelle-nutzen-corona-krise 368531.html

11. Denning, D.E. (1999) Information Warfare and Security. ACM Press, USA
12. Deloitte (2020). Covid-19 and fraud risk: Managing and responding in times of crisis. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/The_Fraud_Triangle_Final.pdf
13. Eboibi, F.E. (2020). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. Commonwealth Law Bulletin 47(1), 113-142. https://doi.org/10.1080/03050718.2020.1834424
14. Ellison, L., & Akdeniz, Y. (1998). Cyberstalking: The Regulation of Harassment on the Internet. Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, pp 29-48.
15. Emmanuel, P. (2021). In 2020, Nigeria lost N5 billion to fraud in 9 Months: What you need to watch for. https://techpoint.africa/2021/02/22/nigeria-lost-5b-fraud-2020/
16. Europol, (2020). Covid-19 sparks upward trend in cybercrime. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
17. Federal Bureau of Investigation (FBI, 2021). Scammers defraud victims millions of Dollars in new trend in romance trend. https://www.ic3.gov/Media/Y2021/PSA210916
18. Financier Worldwide Magazine, (2021, February). Covid-19 fraud outlook. https://www.financierworldwide.com/covid-19-fraud-outlook#.YSxP2Y5KjIU
19. Fruhlinger, J. (2020). What is phishing? How this cyber-attack works and how to prevent it, CSO, 13 February 2020, https://www.csoonline.com/article/2117843/what-isphishing-how-this-cyber-attack-works-and-how-toprevent-it.html.
20. Gordon, S. (2021). What is cyberstalking? https://www.verywellmind.com/what-is-cyberstalking-5181466
21. Govender, I., Watson, B.W.W, and Amra, A. (2021). Global virus lockdown and cybercrime rate trends: a routine activity approach. Journal of Physics: Conference Series Journal of Physics: Conference Series 1828(2021)012107, doi:10.1088/1742-6596/1828/1/012107
22. Groenendaall, J. & Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: A case study. Journal of Contingencies and Crisis Management. 2021; 00:1–6. DOI: 10.1111/1468-5973.12360
23. Hakak, S., Khan, W.Z., Imran, M., Choo, K.-K.R. and Shoaib, M. (2020), "Have you been a victim of COVID-19-Related cyber incidents? Survey, taxonomy and mitigation strategies", IEEE Access, Vol. 8, 124134-124144, doi: 10.1109/ACCESS.2020.3006172.
24. Hakmeh, J., Taylor, E., Peters, E., Ignatidou, S. (2021). The covid-19 pandemic and trends in technology: Transformation in governance and society. International Security Programme, Research Paper.
25. Hassan A. B., Lass F. D. and Makinde J. (2012): Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. 2(7), 626 – 631.
26. Ikechi, K.S & Nwadiubu, A. (2020). Fraud theories and white-collar crimes: Evidence from the Nigerian Banking Industry. International Journal of Management Science and Business Administration 6(6), 25-40. http://dx.doi.org/10.18775/ijmsba.1849-5664-5419.2014.66.1003
27. Interpol 2020 https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats?cv=1
28. International Labour Organisation (ILO, 2021). ILO Monitor: Covid-19 and the world of work. Seventh Edition.https://www.ilo.org/wcmsp5/groups/public/dgreports/dcomm/documents/briefingnote/wcms_767028.pdf
29. Jochims, K. (2020). Covid-19 and cybercrime. https://www.revelock.com/en/blog/covid-19-and-cybercrime .
30. Junger, M., Wang, V. & Schlomers, M. (2020). Fraud against businesses both online and offline: crime scripts, business characteristics, efforts and benefits. Crime Science (2020), 9(13), 1-15. https://doi.org/10.1186/s40163-020-00119-4.
31. Kemp, S., Buil-Gil, D., Moneva, A., Miro-Llinares, F. & Diaz-Castano, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. Journal of Contemporary Criminal Justice 1–22.
32. Kranacher, M.J., Riley, R. and Wells, J.T. (2010), Forensic Accounting and Fraud Examination, John Wiley and Sons, Hoboken, NJ.
33. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computer and Security, 105 June (2021), 102248, arXiv preprint arXiv:2006.11929

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

34. Litan, A. (2004). Phising attack victims likely targets for identity theft. Available: http://www.gartner.com/DisplayDocument?doc_cd=120804
35. Longe, O.B. & Chiemeke, S.C. (2008): Cybercrime and Criminality in Nigeria- What roles are internet access Points in Playing. European Journal of Social Sciences, 6(4),
36. Ma, K.W.F. & Mckinnon, T. (2020). COVID-19 and Cyber Fraud: Emerging threats during the pandemic. York University & Queens University, Ontario Canada.
37. Matthewman, S. & Huppatz, K. (2020) 'A sociology of Covid-19', Journal of Sociology. doi:10.1177/1440783320939416.
38. Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14.
39. Nigerian Communication Commission (NCC, 2016). Effect of cybercrime on foreign direct investment and national development. Department of New Media and information security.
40. Nivette, A. E., Zahnow, R., Aguilar, R., Ahven, A., Amram, S., Ariel, B., Burbano, M. J. A., et al. (2021). A global analysis of the impact of COVID-19 stay-at-home restrictions on crime.. Nature human behaviour, 5 (7), 868-877. https://doi.org/10.1038/s41562-021-01139-z
41. Okereke, O. (2020). Corona virus – the cyber-attack, Cyberattack, 5 February 2020, https://cyberkach.com/2020/02/05/coronavirus/; Pascal Geenens,Coronavirus: Its four most prevalent cyber threats, Radware Blog, 12 March 2020, https://blog.radware.com/security/2020/03/coronavirus-its-four-mostprevalent-cyber-threats/?utm_source=Blog&utm_medium=Gaggle_Twitter&utm_campaign=Social
42. Onaleye, T. (2020). Nigerians suffered 3.8 million malware attacks and 16 million PAU detections in the first seven Month of year 2020.
43. Onozure, D. (2021). Banks lose over N5million to fraudsters in 9 Months – NDIC. https://www.vanguardngr.com/2021/03/banks-lose-over-n5bn-to-fraudsters-in-9-months-ndic/
44. Patterson, D. (2021). Cybercrime in thriving during the pandemic, driven by surge in phishing and ransomware. https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
45. PwC 2020 How to manage the impact of COVID-19 on cyber security. https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-to-manage-the-impact-ofcovid-19-on-cyber-security.html
46. Rachna D., Tygar, J.& Hearst, M. (2006): Why Phishing Works" in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006).
47. Ramamoorti, S. (2008). The Psychology and Sociology of Fraud: Integrating the Behavioural Sciences Component into Fraud and Forensic Accounting Curricula. Issues in Accounting Education 23 (4): 521-533.
48. Roger, E.S. (2008) Rogers Communications Inc, 2008 Annual Report
49. Search security (2009), Information Security magazine
50. Sullivan, M. (2020). As people start working remotely, hackers are trying to exploit our anxieties, Fast Company, 18 March 2020, https://www.fastcompany.com/90478521/as-people-startworking-remotely-hackers-are-trying-to-exploit-ouranxieties
51. Tudor, J. K. (2001) IS security Architecture: An Integrated Approach to Security in the Organization. Auerbach Publications, USA
52. UK Research and Innovation (2021). Fraud during a Pandemic: Identifying and appraising new challenges for the criminal justice response in England and Wales. https://gtr.ukri.org/projects?ref=AH%2FV014781%2F1
53. United Nations Conference on Trade and Development (UNCTAD, 2020). Data and privavy protected in One-third of the countries, despite progress. https://unctad.org/news/data-and-privacy-unprotected-one-third-countries-despite-progress
54. United Nations Office on Drugs and Crimes (UNODC, 2020). Cybercrime and COVID-19: Risks and Responses. https://www.unodc.org/documents/Advocacy-Section/UNODC__CYBERCRIME_AND_COVID19__Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf
55. United Nations Office on Drugs and Crimes (UNODC, 2020). UNODC-ROSA's response to COVID-19: The LEA and Cybercrime Segment. https://www.unodc.org/documents/southasia/UNODC_ROSA_on_Law_Enforcement_COVID_19.pdf
56. Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 74 (12), 38-42.

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

57. World Health Organisation (WHO, 2021). WHO Coronavirus (COVID-19) Dashboard. https://covid19.who.int/