Implication of Cybercrime on Business Operation and Investment in Nigeria

Musa Idris, PhD & Shekinah Oluchukwu Aziagba
Department of Public Administration,
Faculty of Administration,
Ahmadu Bello University, Zaria.
E-mail: Shekinahaziagba@gmaii.com
Phone:+234 706 280 5912

Abstract

Businesses and consumers in Sub-Sahara Africa are facing increasing cyber-threats. The increase in cyber-attacks carried out by malicious cybercriminals taking advantage of a borderless playing field has posed as an obstacle to society's continued path to development. Specific key cyber-threats worldwide includes financial crimes, cyber-terrorism, cyber conflict, cyber espionage, child online abuse and exploitation among others. These cyber-attacks can be attributed to vulnerable systems and lax cybersecurity practices threatening lives, crippling businesses and having in itself the capacity to scare off foreign direct investment. The paper seeks to determine the implications of cybercrime on business operations and investment in Nigeria. The study relied on secondary sources of data and analyzed the data using content analysis. The study identified poor security system as one of the major leading factors associated with cybercrimes. The high cost associated with maintaining a strong security system lias kept many organizations operating below the security poverty line from adequately protecting themselves against losses. The paper therefore recommends among others the fortification of national infrastructure by the government. The strengthening of cybersecurity measures will help prevent cyber-threats from undermining the stability of information societies thereby enabling digital technologies to become a source of development instead of a source of risk.

Keywords: Cybersecurity, security threats, cybercrime, business operations, investment, Nigeria.

Introduction

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet (Okeshola & Adeta, 2013). The cyberspace has provided an internet platform which has enabled geometric growth, productivity, efficiency and accelerated windows of opportunities for businesses and the removal of economic barriers hitherto faced by corporate organizations across the globe (Okpa, Adebayo & Emmanuel, 2020). Organizations from various part of the world can now freely access and utilize the comfort, convenience, ease, productivity and efficiency offered by the internet platform in their daily interactions with one another (Abdul-Rasheed, Lateef, Yinusa & Abdullateef, 2016). The advent of internet and the adoption and evolution of new technologies and products have made it easier for organizations, businesses and consumers to operate on a larger dimension, while enabling groups and individuals to be active participants in the global economy (ICSPA, 2016). There is no gainsaying the fact that the internet has proven to be one of the most efficient ways of transacting business in the 21st century, despite the risks involved.

Ironically, this technological revolution has evolved to become a smart instrument used by criminal elements for various forms of fraudulent and criminal activities. Accordingly, Shehu (2014) posits that the convergence of computing and communications, and the rapid growth of digital technology have brought immense benefits to society, but these benefits also come with greater risks both nationally and internationally. Today, many traditional crimes are now being aided or abetted through the use of computers and networks, and wrongdoing previously never

imagined has surfaced because of the incredible capacities of the information system. Okeshola and Adeta (2013) avers that the information technology revolution associated with the internet has brought about two edge functions: that is on one hand, it has contributed positive values to the world; while on the other hand, it has produced so many maladies that threaten the order of the society and also producing a new wave of crime to the world.

It is observed that, among the copious misdemeanors committed daily, using modern telecommunication networks, Nigeria and some other developing countries like South Africa, Tanzania, Ghana, Egypt, Kenya, Rwanda, Uganda, among others are alleged to be at the forefront, particularly, with reference to sending deceitful, deceptive and spurious financial proposals all over the world (Longe, Mbarika, Kourouma, Wada & Isabalija, 2009). Nigeria is without doubt one of the most enterprising locations in Africa, boasting the largest population of all the countries on the continent and an economy that surpasses those of neighboring states. While there are signs of Nigeria developing into a major global economy, certain steps must be taken rapidly to thwart the risk of damage to businesses resulting from catastrophic cyberattacks (Securex, 2019). According to statistics, the estimated annual cost of cybercrime in Nigeria already amounts to approximately 0.08% of the country's Gross Domestic Products (GDP), with Ransomware just one of the major threats gathering momentum (Securex, 2019).

Today, in comparison to physical space, cyberspace is virtually ubiquitous, operationally more efficient, socio-politically more vibrant, economically as resourceful, and information-wise more integrated. Given its ubiquity, scale and scope, cyberspace has become a fundamental feature of the world we live in. In the developed world, cyberspace is well patronized; while, in the developing world, it is becoming increasingly patronized. Due to all these realities, crime and criminality have also moved into cyberspace with increasing sophistication. Cybercrime and attacks are on the increase and it appears the internet is no longer safe, considering the emerging threats and the number of attacks being recorded daily. Today, we are being faced with a series of challenges such as Ransom-ware, Virus, Trojans, Phishing, Spyware, Mal-advertising, Man in the Middle, Man in the Browser, Hacking, Spoofing, Denial of Service, Distributed Denial of Service attacks, Website defacement, Cyber espionage, Pharming, Cyber terrorism, Internet of Things (IoT) and many more (Anyawu, 2018).

The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the economy of the country is highly disturbing (Ibikunle & Eweniyi, 2013). It is not unusual to hear that despite its many benefits cyberspace has, at the same time, opened doors for those intent on achieving criminal aims. Cyber blackmail, identity theft and fraud are some of the ways in which these have been previously witnessed (Irandoost, 2018). In a recent *Worldwide Threat Assessment of the US Intelligence Community* (2016), 'Cyber and Technology' was put as the top priority ahead of other prominent threats including terrorism, the proliferation of weapons of mass destruction and counterintelligence. Compared to a decade ago – and before – when cyber and technology were at the bottom of this list, this is an alarming development that begs significant attention (Lyngaas, 2016 cited in Irandoost, 2018).

Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users (Ibikunle & Eweniyi, 2013). Prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet (Moses-Oke, 2012).

Since then, and with internet penetration globally at an estimated 3.4 billion users (approximately 46% of the world's population), the opportunities for cybercrime have ballooned exponentially (ACS, 2016). There are the costs incurred by the government due to the rise of cyber-crime. As for measuring costs, the Detica report considered four categories: costs in anticipation of cybercrime, such as antivirus software, insurance and compliance; costs as a

consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise; costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies; indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy (Anderson, 2012).

It turns out that Nigeria is one of the world's most vulnerable countries to cyber-attacks – 16th worst in the world in 2016, an improvement from 2nd the year before. In 2018 alone, about 60% of Nigerian firms suffered an attack, and spent about $270million on cybersecurity. Nigerian firms are being attacked but no one is reporting what is stolen. Despite spending good money on cybersecurity, Nigerian companies reportedly lost "billions" of naira to cyber-attacks (World Bank, 2020). Increasing cyber-attacks in the continent can be attributed to vulnerable systems and lax cybersecurity practices (Kshetri, 2019). Hardly a day goes by without news regarding cybersecurity threats. Whether it is about elections, e-commerce, business, or social media threats – digital systems are growing, which creates both challenges and opportunities for business development (Damicis, 2019).

There are numerous risks that organizations engaged in e-commerce face, such as financial, legal, supply chain, safety, and security. The security risk presents several components or dimensions, one of the most concerning is the cybersecurity risk (Vasiu & Vasiu, 2018). The high level of inter-connectivity, which characterizes modern society and the international trade, has opened many avenues for cyber-attacks, rendering cybersecurity an issue of major concern for all organizations (World Economic Forum, 2018). Even though, in recent years, there were notable advances in the understanding and mitigation of cyber risks, as empirical data shows, the number of incidents augmented and continued to grow in sophistication, becoming more thorough and inflicting often major losses (IDG, 2017). Through advanced tools, tactics and procedures (TTP), such as SQL injection; malware infection; advertisement click fraud; business e-mail compromise (BEC); and exploitation of zero-day vulnerabilities, used in watering hole attacks, cyber criminals pose major threats to organizations and citizens. Cyber incidents have the potential to very negatively affect organizations' activity, economic development, and users' privacy and other fundamental rights (Vasiu &Vasiu, 2018).

It does not come as a surprise, therefore, that the value of the cybersecurity market is estimated to grow from $120 billion in 2019 to $300 billion by 2024. It is more surprising that, while efforts and investment to improve cybersecurity continue to grow, security developments lag behind the pace of the malicious use of digital technologies. Cyber threats are escalating in frequency, impact and sophistication. The World Economic Forum's Global Risks Report 2019 ranked cybercrime among the top-five risks. At a global level, cybercrime causes multibillion dollar losses to business; the average cost of cybercrime for an organization has increased from $11.7 million in 2017 to $13.0 million (Taddeo & Bosco, 2019). According to the 2018 Africa Cyber Threat Intelligence Report (ACTIR), more than 90% of African businesses were operating below the cybersecurity "poverty line" – meaning they couldn't adequately protect themselves against losses.

Nigeria currently loses about NGN 78 billion annually to the activities of cyber criminals whose major targets are financial institutions, government ministries, departments and agencies as well as their affiliates (Anyanwu, 2018). The cost of malicious cyber activity involves more than the loss of financial assets or intellectual property. There are opportunity costs, damage to brand and reputation, consumer losses from fraud, the opportunity costs of service disruptions "cleaning up" after cyber incidents, and the cost of increased spending on mitigating cybercrimes (McAfee, 2013). Companies have to rethink how they collect and store information to ensure that sensitive information isn't vulnerable. Many companies have stopped storing customers' financial and personal information, such as credit card numbers, social security numbers and birth dates. Some companies have shut down their online stores out of concern that they cannot adequately protect against cyber-theft (Mohr, 2019).

Cybersecurity experts have decried the level of preparedness of Nigerian organizations against cyber-attacks as a follow-up to a recent cyber security report which finds that over 90% of

Nigerian organizations are operating below the security poverty line significantly exposing themselves to cyber security risks (Onwuegbuchi, 2018).The vulnerability of Nigeria's cyberspace to different dimensions of cybercrime has added a new twist to the country's economic development conundrum. It is to this end that this paper seeks to answer the question, to what extent has cybercrime affected business operations and investment in Nigeria. The objective of the study is to determine the implications of cybercrime on business operations and investment in Nigeria.

Conceptual Clarifications

The two basic concepts that constitute the conceptual thrust of this paper are business operations and investment. Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. Generally, cybercrime may be divided into one of two types of categories: crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, malware etc., and crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples includes cyber stalking, fraud and identity theft, phishing scams and information warfare (Omodunbi, Odiase, Olaniyan and Esan, 2016). Cyber-crime therefore refers to criminal activity perpetrated in the cyber space through the medium of computers and the internet.

The world of business operations can be so vast, complicated, and at times, vague, that it can be hard to pinpoint what exactly the term "business operations" means. Business operations function as an overarching plan or map for your business. From investors to executives to employees, operations involve every aspect of operating a business (Browne, 2019). Business Operations refers to activities that businesses engage in on a daily basis to increase the value of the enterprise and earn a profit. The activities can be optimized to generate sufficient revenues to cover expenses and earn a profit for the owners of the business (Corporate Finance Institute, 2015). The National Computer Security Survey (NCSS) in 2005 found that 67% if surveyed businesses had discovered at least one form of cybercrime. There is no relief in sight for businesses beleaguered with cyber-crime, or those fighting against it. Protecting the business against incursion is costly and can impact the relationship between the company and its customers. As cyber-crime becomes more sophisticated, business will have to stay one step ahead (Mohr, 2019).

An investment always concerns the outlay of some asset today–time, money, or effort–in hopes of a greater payoff in the future than what was originally put in. An investment can refer to any mechanism used for generating future income. Investment is an asset or item acquired with the goal of generating income or appreciation. When an individual purchases a good as an investment, the intent is not to consume the good but rather to use it in the future to create wealth (Chen, 2020). An investing company may make its overseas investment in a number of ways - either by setting up a subsidiary or associate company in the foreign country, by acquiring shares of an overseas company, or through a merger or joint venture (NCC, 2017).Financially speaking, an investment means an asset that is obtained with the intention of allowing it to appreciate in value over time.

Methodology

This study being a desk or library research, relied entirely on secondary data comprising scholarly peer-reviewed journal articles, books, newspaper reports, and relevant materials downloaded from the internet. The data were content analyzed and presented thematically.

Factors behind Emerging Security Threats

Nigeria's cyberspace is characterized by high risk exposure. This is evident in the extent of threat and vulnerability to which the domain is exposed. The cause and drivers of cyber malaise in Nigeria are systemic and various. According to Nnamani (2016) and Adesina (2017), these malaise can be attributed to the rising poverty levels, greed (of both perpetrators and sometimes even the victims), and easy access to gullible targets by criminals, and lack of adequate legal and

regulatory policies to prevent and prosecute the perpetrators. Economic hardship, accentuated by lack of employment and safety nets, has provided material incentive for criminal indulgence and franchise among the youths.

Weak Legislation and Law Enforcement

Most African economies are characterized by permissiveness of regulatory regimes that provide a fertile ground for cybercrime activities. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. For instance, it was reported that government officials in Nigeria claimed that they were ignorant of cybercrimes originated from the country and some labeled it as Western propaganda. Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives for his alleged engagement in cybercrime-related activities (Kshetri, 2013).

Cybercriminals also benefit from inter-jurisdictional and intra-jurisdictional arbitrage. Following raids on cyber cafés in major cities in Nigeria, cybercriminals were reported to move to remote areas to carry out their operations. The porous national borders and a lack of states' controls on their territories mean that cybercriminals can easily migrate from one jurisdiction to another with a weaker rule of law and enforcement. A Barrister of Nigeria's Economic and Financial Crimes Commission (EFCC) noted that when Nigeria strengthened its anti-cybercrime measures, cybercriminals were leaving the country and moving to other West African countries (Kshetri, 2019).

Economic Hardship/Poor Governance

It is an obvious datum that despite Nigeria's vast resources and huge potentialities, she remains grossly undeveloped as abject poverty, acute youth unemployment; heightened crime rate, poor health prospects and widespread malnourishment have been the main features of Nigeria's political economy (Ogundiya 2010 cited in Anyadike & Emeh, 2014). Hence, the problem of development in Nigeria is a problem of governance; especially when defined in terms of the proper, fair and equitable allocation of resources for the achievement of the ends of the state, which is the promotion of the common good of the people. Not to mention most importantly the fact that, Nigeria has been categorized among countries practicing all manners of online fraud such as hacking, fraudulent transactions via the internet, theft of credit cards among others, although, this categorization does not augur well with the country (Fayomi et al, 2015).

It has been noted that economic hardship/deprivation influences people to resort to illegal means of meeting their daily needs. In 2015, the UN identified 17 Sustainable Development Goals (SDGs) to be achieved by 2030 – ranging from eradicating poverty and guaranteeing stability and peace to fighting discrimination and climate change. Digital technologies, particularly the internet of things (IoT) and artificial intelligence (AI), can facilitate efforts to achieve the SDGs. For example, AI can help detect malnutrition using photographs of individuals living in a given area. Here too, cybersecurity is crucial. Should pictures of those individuals be stolen or the AI model become corrupted, the use of AI to fight starvation would become problematic. Cybersecurity underpins trust in, and thus the adoption of, digital technologies for humanitarian and environmental purposes (Taddeo & Bosco, 2019).

Unemployment

This is a serious threat to Nigeria's development generally. Most of the crimes occur as a result of the high rate of unemployment. Low levels of income and education lead to relative laggardness in developing world-based businesses' and consumers' adoption of new technologies. Many Internet users in the developing world are inexperienced and not technically savvy as a high proportion of them got their computers and connected to the Internet not long ago (Kshetri, 2010). Cyber-crime has thrown up emergency millionaires or billionaires in Nigeria which is injurious to

the economic development of the country as most of such funds acquired illegally are not been used productively to promote the economy of the nation. The crime has diverted the attention of so many Nigerian youth from undertaking productive activities such as manufacturing, construction as well as large scale farming that would have grown the economy to such criminal activities because of the flamboyant life chances and life styles that it presents (Okeshola & Adeta, 2013).

Nigerian youth accounts for about 43% of our 178.5 million estimated population. Sadly, about 25% of them are either unemployed or underemployed because their education and skill training is inadequate to meet the demands of modern-day challenges. This limitation poses a great challenge (Anyanwu, 2018). The Issue of cybercrime and its impact on the Nigerian economy has increasingly become worrisome and has seen an increase in the unemployment rating of the country. As the rate of unemployment increases and cybercrime continues, parent companies are seen fleeing the country in a bid to secure their investments, while some cut their staff strength due to cybercrime that has led to fall in their profit.

Corruption/Fraud

This hampers economic growth, disproportionately burdens the poor and undermines the effectiveness of investment and aid. The impact of cybercrime already has a detrimental influence on Nigerian Citizenry/Economy. According to the 2019 Corruption Perceptions Index reported by Transparency International, Nigeria is the 146 least corrupt nation out of 180.Businessamlive (2019), avers that Nigeria is losing trillions to corruption. Forensic experts alleged growing cases of fraud, cybercrime and corruption in the country. Despite government's renewed efforts to address these problems, very little result has been achieved, especially in the area of securing conviction against perpetrators of fraud in Nigeria because many of the cases, especially the high-profile ones are either thrown out or want of evidence or are unnecessarily delayed and stuck in court for years due to one reason or the other.

The prevalence of cybercrime has also created a bad image for Nigeria amongst the committee of nations as one of the most corrupt nations in the world. This dent on the national image affects the way her citizens are treated abroad. They are related to with suspicion and extreme caution, hence not to be trusted. Ene et al (2016), observed that the activities of Nigeria's popular "yahoo boys" have created a bad image for the country as information coming from Nigeria is frequently regarded as a scam. This means that Mails from Nigeria's financial institutions may not get full attention, and may likely be considered a scam because of how people outside the country see Nigerians as criminals. Nigerians may soon be undergoing serious scrutiny when establishing a business in another country, more serious than what it is experiencing now if at all are not met with total denial.

Cybersecurity Risks Faced by Organizations

There are numerous risks that organizations engaged in e-commerce face, such as financial, legal, supply chain, safety, and security. The security risk presents several dimensions, one of which is the cybersecurity risk. Some of the main cybersecurity risks faced by e-commerce organizations includes; damage, trade secret theft, and payment fraud.

Damage: Computer data is essential for the proper functioning of organizations. Successful damage or impairment attacks can negatively impact the integrity and availability of data and/or information systems. Whether in the form of impairment, sabotage, subversion, or intrusion, these attacks can inflict direct and proximate harm on a significant scale (Vasiu & Vasiu, 2018). This fact is reflected in a recent survey of business continuity professionals from 80 countries, which identified "cyberattacks" as the fourth most significant cause of business disruption, while "data breach" was ranked the ninth most important source of disruption (Business Continuity Institute, 2017). While the intent and motive that drive damage attacks vary significantly, often the motivation is represented by revenge or retaliation (Vasiu & Vasiu, 2014). Such malicious acts or actions, nevertheless, can have behind hacktivism, the perpetration of other crimes, usually to derive profit, or the attempt to cover, render untraceable or unrecoverable incriminating evidence of previously perpetrated offenses (Vasiu & Vasiu, 2014).

Theft of Trade Secrets: Trade secret protection broadly encompasses the following categories: technical data; confidential business information, including clients' contact information, pricing information, prior purchase history, product preferences and habits; and know-how. The theft of trade secrets is wide-spread, overall, according to estimates, the theft of trade secrets costs up to $300 billion per year (Almeling et al, 2010). Misappropriation of trade secrets can take the form of economic espionage, which benefits a foreign state or instrumentality, and theft for pecuniary gain, which benefits an individual or an organization (Vasiu & Vasiu, 2017). This threat come from numerous sources, such as current or former employees, competitors, clients, suppliers, and hackers (Vasiu & Vasiu, 2017). The theft of trade secrets affects all major economic sectors, and can result in very significant economic and other harm to the owner of the trade secret, as well as to others. Successful or attempted trade secret theft may result in loss of sales, costs for internal investigation, negotiating settlements, prosecution and litigation, and higher disbursement for security measures.

Payment Fraud: The main category of proceeds-generating crime on the Internet as in the real world is fraud, that is, the intentional deception causing loss of property to another person for economic gain (Council of Europe, 2012 cited in Vasiu & Vasiu, 2018). Financial gain is by far the most powerful motivation behind payment frauds, however, these offenses can also be encountered as hacktivism (Vasiu & Vasiu, 2014). Financial losses, due to cyber heist or fraud, can be massive, and can affect organizations from all industries, particularly the banking sector. For instance, the Carbanak group, targeted hundreds of banks, in several countries, the total amount stolen being estimated at $1 billion. The Banswift group, by exploiting weaknesses in bank's security, infiltrated the network and obtained transaction credentials, managing to steal $81 million from Bangladesh's central bank (Symantec Corporation, 2017). In another recent major case, roughly 500,000 computers were infected globally with malware, conceived to obtain victims' sensitive banking credentials, with a view to conduct fraudulent wire transfers (U.S. Department of Justice, 2016).

Implications of Nigeria's Cyber Menace for Business and Investment

The cost of cybercrime to a society can be both qualitative and non-qualitative. The implications of Nigeria's cyber menace on business and investment is categorized into two; implications for potential business investment, and implications for existing enterprises/organizations.

Potential Business Investment

The growth and development of Africa and indeed Nigeria's economy depends largely on Foreign Direct Investments (FDI), which has been described as the major carrier for the transfer of new scientific knowledge and related technological innovations. Nigeria is one of the economies with great demand for goods and services and has attracted some FDI over the past years (NCC, 2017). Recently, the flow of investment into the country has been declining due to issues in the economy, which have made Nigeria not to be the "darling" of foreign investors anymore. The Nigerian economy recorded a total decline of $11.68bn (N2.3tn) in investment inflow in the last three years. Since 2013, the country has been experiencing persistent decline in the value of direct and portfolio investments (NCC, 2017).This problem has been attributed to continued cyber-attacks on foreign investors in the country which has since succeeded in scaring away foreign investors and discouraging others from coming to invest in Nigeria. This means that there will be continuous less inflow of funds which may directly affect social and economic development in the country (Epron, 2019).

In a study by World Bank on investment climate in nine African countries, it was found that 29% of business operators in Africa and 36% in Nigeria perceived insecurity as a major constraint on investment. This situation has the damaging consequence of giving signal to the international community that Nigeria is not a safe and secure place and as such not suitable for investment and business activities. In that case, foreign firms and entrepreneurs would decline to invest and this is particularly important in view of the efforts being made to create the desired

atmosphere to attract foreign direct investment. So, it is a strong disincentive to business investment as it scares away potential investors. This is because such environments or economies are considered high risk zones due to the high level of uncertainty about the safety of investment and lives of the managers and their staff (Ujah & Eboh, 2006).The financial cost of cyber-crimes constitutes a huge economic waste. Beyond the economic waste are critical opportunity costs, such as unfavorable investment and business climate. The persistence of cybercrime has been one of the most critical dimensions negating economic development in Nigeria.

Existing Business Enterprise/Organizations

Cybercrime has the capacity of halting business operations and or the closure of many enterprises. Because many organizations are operating below the poverty line, they lack the capacity to protect themselves against the risks and losses associated with cybercrimes. According to Heli (2011), the majority of attacks at this level are carried out for economic gains and with criminal motives. In some sectors where cybercrime has been active for a long time, smaller companies are already heavily burdened by losses occurring from data theft and from additional administrative measures that should be applied to protect their clients' personal information or assets. Vasiu and Vasiu (2018) observed that the most obvious results of cybersecurity incidents are financial losses, however, cyber incidents can also result in costly recovery or remediation and, in certain cases, litigation; serious harm to consumers' privacy, resulting in potential fines, imposed on the basis of regulations, such as the General Data Protection Regulation (GDPR), which can amount to 20 million euros or 4% percent of an organization's worldwide turnover; impaired organizational operational integrity, infringement of intellectual property rights, and bad reputation.

Cyber incidents can also very negatively affect "trust", a very important social capital indicator and a determining factor of economic growth (Hamilton, 2006). As Oliveira et al. (2017) explain, "firm characteristics (reputation and brand recognition), lack of integrity, privacy and security and likability (website infrastructure), and interactions (service quality and customer satisfaction), are the major sources of trust that influence the three dimensions of consumer trust, namely: competence, integrity and benevolence; which explains that overall trust has a direct effect on intention to purchase online." According to Savaglia and Wang (2017), the ability to manage the cybersecurity risk is essential for organizations' success. In order to effectively be part of the solution to cyber risks, it is imperative that organizations make extensive vulnerability or weakness analysis mandatory.

Human negligence and inadequate level of e-skills have originated at least as much security breaches in organizations as have external attacks. Companies in the financial sector are already investing into anti-fraud systems, and are used to bearing the consequences of the successful crime attempts. Other companies are securing their systems for preserving sensitive business information and preventing the loss of corporate secrets (Heli, 2011). In cases where customers records are compromised by a security breach associated with cybercrime, a company's reputation can take a major hit. Customers whose credit card or other financial data become intercepted by hackers or other infiltrators lose confidence in such an organization and often begin taking their business elsewhere (Igba et al, 2018).Cybersecurity measures must commensurate with the level of risks identified.

Conclusion and Recommendation

Just like a virus, the menace of cybercrime has eaten deep into the fabrics of our society and poses threats to the economic development of the country. Although cybercrime is a global phenomenon, the vulnerabilities and impact trends do tend to differ depending on the strength of the measures each country put in place to combat the threat such as cyber laws and cyber protection technologies. Nigeria's economic development has been hampered by these emerging threats – cybercrime among others. The causes of cybersecurity incidents are numerous and multifaceted. Successful cyber-attacks are usually the result of various problems, such as software vulnerabilities, poor authentication, exploitation of trust mechanisms, insufficient awareness of cybersecurity risks, or administrative errors.

The adoption of ICT is changing virtually every aspects of our lives and significantly contributing to the achievement of the United Nations' 2030 SDGs. However, these benefits of ICT comes at a cost, namely cybersecurity risk. Organizations face numerous types of cybersecurity incidents. This paper outlined some of the main cybersecurity risks faced by Organizations and individuals and its implication on economic development. Our society today depends so much on technology. Just as technology brings great benefits, it also brings great threat, by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyber-attacks. Cybercrime can very negatively impact the fundamental security attributes of integrity, availability, and confidentiality, resulting in disrupted or delayed services or activities, financial loss, and overall distrust in electronic transactions.

In order to keep our way of life and to continue to prosper through technology, we must ensure that technology always operates and works for us as intended. Therefore, protecting it is of paramount priority. Cybercrimes continue to evolve and, in order to keep data and systems in a protected state, significant and effective measure must be taken in order to have a truly effective approach. The paper therefore recommends the following:

i. Cybersecurity is not only about technological defences, it is also about people. Everyone needs a basic understanding of cyber threats and how to recognize them – something which comes under the umbrella of digital literacy. Therefore, to improve cybersecurity, there is need to provide widely public awareness training and assistance in information security, as well as effective law enforcement which will be able to cope with destructive campaigns on the internet. There is also need for organizations to work with the right agency to put in place legal and regulatory framework that will ensure prosecution and punishment of cybercriminals. Better public awareness of all computer users, will contribute to the prevention of identity thefts and will decrease the number of people and companies targeted by malicious activities in the internet. In this regard, all individuals have a great role to play in creating a more secure information society in the long run.

ii. To strengthen the security of economic actors, government can direct more resources for the fight against cybercrime through the development of specific cybersecurity program across all sectors of the society that will take into consideration the peculiarities of the Nigerian environment and unique threats being faced. These programmes should be targeted at training and educating the information technology workforce and guaranteeing that companies have an environment where it is safe to operate. As an essential resource of information societies, the improvement of cybersecurity in Nigeria will help foster societal and economic development.

iii. To curtail cyber-attacks, the fortification of national infrastructure against cyber-attacks by government is of paramount necessity. Without effective security measures in place, cyberthreats may undermine the stability of information societies, which will cause digital technologies to become a source of risk instead of a source of development. Upon the discovery that the majority of the infrastructure is owned by the private sector and the majority of actors in cyberspace are companies and individuals, government need to create effective public-private partnerships for securing cyberspace. The most effective response by governments could be to provide support for critical civilian infrastructure and to build a national cyber system that is resilient in times of crisis.

Reference

Abdul-Rasheed, S.L., Lateef, I., Yinusa, M.A., and Abdullateef, R. (2016). Cybercrime and Nigeria's External Image: A Critical Assessment. *Journal of Pan African Studies*, 9: 119-132.

Adesina, S.O. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, 13(4), 19-29.

ACS (2016). Cybersecurity Guide: Threats, Challenges, Opportunities.

ACTIR (2018). The 2018 Africa Cyber Threat Intelligence Report.

Almeling, D.S., Snyder, S.W., Sapoznikow, M., McCollum, W.E., & Weader, J. (2010). A Statistical Analysis of Trade Secret Litigation in Federal Courts. *Gonzaga Law Review*, 45:291-334.

Anderson, Ross, et al. (2012): Measuring the Cost of Cybercrime, 11th Workshop on the Economics of Information Security held on June 2012.

Anyadike, N.O and Emeh, I.E.J (2014).Effective Leadership for Good Governance in Nigeria; Addressing the Interface. *Journal of Humanities and Social Science*, 19(1), 69-74.

Anyanwu, L.O. (2018). Safe Computing for Emerging Economies. Cambridge Scholars Publishing. Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK.

Browne, R. (2019, July 25). *A Business Operations Definition and Complete Guide in 31 Terms*. Learning Hub.

Businessamlive (2019). Cyber-Security: Nigeria is Losing Trillions to Corruption, Say Forensic Expert.

CFI (2015). *Business Operations – Overview, Examples, How to Improve*. Corporate Finance Institute.

Chen, J. (2020, September 2). *Investing Essentials*. Investopedia.

Damicis J. (2019) Recent and Emerging Trends in Cybersecurity for Economic and Business Development.

Epron, S. (2019). Emerging Security Threats: Factors and Implications for Nigeria's Socio-Economic Development 2015-2019. *Journal of Economics and Development Studies*,7(9), 141-149.

Fayomi, O., Ndubisi, O.N., Ayo, C., Chidozie, F., Ajayi, L., and Okorie, U. (2015), Cyber-Attack as a Menace to Effective Governance in Nigeria. 107-116.

Hamilton, K. (2006). Where is the Wealth of Nations?: Measuring Capital for the 21st Century. World Bank Publications.

HeliTiirmaa-Klaar (2011). Cyber Security Threats and Responses: At Global, Nation-State, Industry and Individual Levels – Mars 2011

Ibikunle, F. and Eweniyi, O. (2013). Approach to Cybersecurity Issues in Nigeria: Challenges and Solution, *International Journal of Cognitive Research in Science, Engineering and Education, 1(1),*

ICSPA, (2016). A Study on the Impact of Cybercrime on Businesses in Canada. The International Cyber Security Protection Alliance (ICSPA), Buckinghamshire, UK.

IDG (2017). 2017 U.S. State of Cybercrime.

Igba, D.I., Igba, E.C., Nwambam, A.S., Nnamani, S.C., Egbe, E.U., and Ogodo, J.V. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. *International Journal of Applied Engineering Research*, 13(2), 1144-1154.

Irandoost, D.H. (2018). Cybersecurity: A National Security Issue?

Kshetri N. (2019) Cybercrime and Cybersecurity in Africa, *Journal of Global Information Technology Management*, 22(2), 77-81.

Kshetri, N. (2016). Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. *Crime, Law and Social Change*, 66 (3), 313–338.

Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Basingstoke, U.K: Palgrave Macmillan: Houndmills.

Longe, B.O., Mbarika, V., Kourouma, M., Wada, F. and Isabalija, R. (2009). Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. *International Journal of Computer Science Information Security*, 6:124-135.

McAfee (2013). *The Economic Impact of Cybercrime and Cyber Espionage*. Center for Strategic and International Studies.

Mohr, A. (2019, June 25). *3 Ways Cyber-Crime Impacts Business*. Investopedia.

Moses-Òkè, R.O. (2012): Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology, *Journal of Philosophy, Science and Law*, 12.

NCC (2017). Final Report on: Effects of Cyber Crime on Foreign Direct Investment and National Development. *Nigerian Communications Commission.*

Nnamani, I. (2016). 'Foreword'. *Nigeria Cyber Security Report2016*. Serianu Ltd.

Oliveira, T., Alhinho, M., Rita, P., & Dhillon, G. (2017). Modelling and Testing Consumer Trust Dimensions in e-commerce. *Computers in Human Behavior*, 71:153-164.

Okpa, J.T., Adebayo, A.I., and Emmanuel, E. (2020). Cybercrime and Socio-Economic Development of Corporate Organizations in Cross River State, Nigeria. *Asian Journal of Scientific Research*, 13(3), 205-213.

Okeshola, F.B. and Adeta, A.K. (2013): The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), 99-114.

Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M., and Esan, A.O (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology*, 1(1), 37-45.

Onwuegbuchi C. (2018, August). Experts worry over rising Cyber Security Poverty Line in Nigeria. *The Guardian*

Savaglia, J. & Wang, P. (2017). Cybersecurity vulnerability analysis via virtualization. *Issues in Information Systems, 18(4)*, 91-98.

Securex West Africa (2019, November 16th). Cybersecurity in Nigeria Needs to be a Priority and here's why.

Schaeffer, B. S., et al. (2009): Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others

Shehu A.Y (2014): Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research*, 3(7), 169-180.

Symantec Corporation (2017). Internet Security Threat Report.

Taddeo, M. and Bosco, F. (2019). *We Must Treat Cybersecurity as a Public Good. Here's WHY*. World Economic Forum Centre for Cybersecurity.

U.S. Department of Justice (2016). Avalanche Network Dismantled in International Cyber Operation.

Vasiu, I., & Vasiu, L. (2014). Break on Through: An Analysis of Computer Damage Cases. *Pittsburgh Journal of Technology Law & Policy, 14*: 158-201.

Vasiu, I., &Vasiu, L. (2017). Backdoor Man: A Radiograph of Computer Source Code Theft Cases. *Journal of High Technology Law, 18(1)*, 1-37.

Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. *European Journal of Sustainable Development, 7(4)*, 171-178.

World Bank. (2020). Nigeria's Cybersecurity Problem

World Economic Forum (2018). The Global Risks Report 2018.