THE IMPACT OF CYBERCRIME ON THE NIGERIAN ECONOMY AND BANKING SYSTEM

BY UMARU IBRAHIM, FCIB, mni,

1.0 Introduction

The role that Information and Communication Technology (ICT) plays in all aspects of human endeavors is well documented and evident. ICT has integrated different economies of the world, through the aid of electronics via the internet. Many corporate organizations, including banks now depend on ICT and computer networks to perform basic as well as complex tasks. The electronic market is now open to everybody, including criminals. It is projected that by 2020, global Cyber security spending will reach $170bn, a 126% increase from $75bn in 2015.

According to the World Economic Forum's report Globalization 4.0, "More organizations than ever are conducting business online" (Davos 2019). The spate of rising preponderance of digital footprints and sophistication in cyber-attacks has prompted the urgency to intensely secure data and other organizational resources from exposure to activities of cybercriminals. This has been the reason for increasing cost of deploying ICT within institutions due to added costs of enhancing security from cyber-attacks.

On this backdrop, Gartner[1] predicted that worldwide spending on information security will significantly grow to $124 billion in 2019. And still, spending according to some security researchers estimate that cybercrime costs will quadruple from its figure in 2015 to about $2.1 trillion by end-2019, and outpace expenditure on cyber-security by over 16 times. The vulnerability of this electronic market to criminal activities has therefore been a growing concern.

Nigeria's internet penetration since the 21st century had been on the increase. Internet users as a percentage of the population increased significantly from 3.5% in 2005 to 47.4% in 2014 (WDI, 2016). Similarly, tele-density has been forecasted to continuously increase overtime in Nigeria (Asemota, et al, 2015). The proliferation of internet in Nigeria has indeed come with unintended consequence, as a haven for criminals. Cybercrime has remained a challenging issue despite increasing awareness and attention to addressing the menace in Nigeria and across the globe. For instance, Cybercrime accounted for about 43% of total monetary loss due to fraud in 2016.

These losses have negative impacts on individuals, businesses and the government in terms of welfare losses, business disruption, profit reduction/rising operating cost and revenue losses, etc. Rising interconnectedness among countries and the use of electronic devices to ease financial and trade transactions call for increased regulation

[1] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

and check on illegal activities associated with technological advancement.

The introduction of Crypto currency, a novel form of technology platform for trading virtual currencies and carrying out other transactions confirms the rapid global technological expansion and the need to regulate these activities. Despite the relevance of this topic to economic development and financial stability, there is scarce literature on it, particularly in Nigeria. This study therefore aims to add to the Nigerian literature, thus providing guidance for policy makers. The objective of this study is to conceptualize cybercrime, identify its causes and impacts on the Nigerian economy as well as proffer strategies to nip it in the bud.

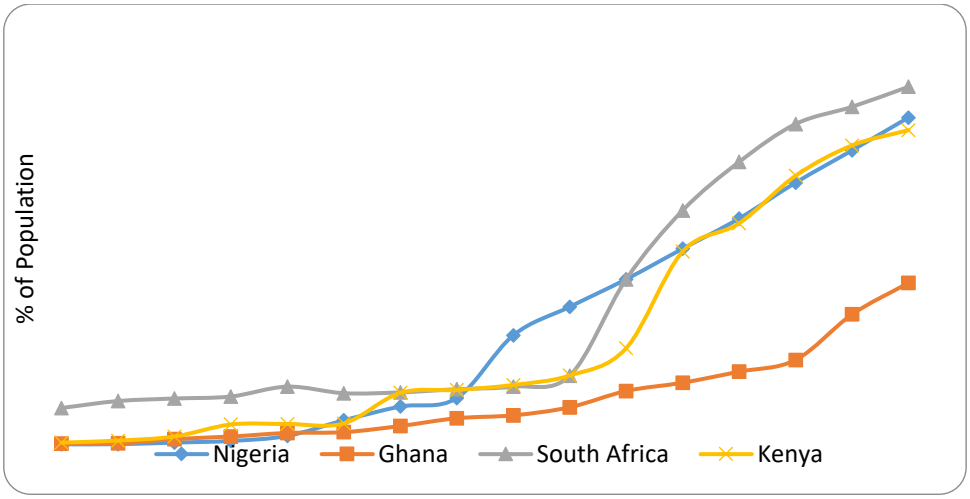
The rest of the paper is structured into 6 sections. Thus, apart from this introduction, Section 2 documents stylized facts on Information and Communication Technology (ICT) in Nigeria. Section 3 focuses on conceptual issues, while Section 4 discusses the causes and effects of cybercrime in Nigeria. Section 5 examines its impacts on the Nigerian economy and banking system and Section 6 proffers strategies for addressing cybercrime in the banking industry. Section 7 concludes the paper.

2.0 Stylized Facts on Information and Communication Technology (ICT) Performance in Nigeria.

Cybercrimes are perpetrated leveraging the internet, and advancement in ICT could provide a handy tool for the proliferation of criminal activities, if not properly regulated. Nigeria has achieved great feats in ICT development, particularly over the last decade and half. To put these achievements in perspective and to also measure her performance, a comparative analysis of Nigeria with her African peers is germane. This is the main objective of this section.

Figure 1 shows internet usage in Nigeria, Ghana, South Africa and Kenya, as a percentage of population. These countries were chosen based on the size of their economies (GDP) and development of their financial sector, thus necessitating greater use of ICT. There are two main inferences discernible from the chart.

Figure 1: Users of Internet (percentage of population)



Source: World Development Indicators (2016)

The first is the significant rise in the population with access to internet facilities between 2011 and 2015 in all the countries. The increase was particularly greater for Nigeria, South Africa and Kenya. The second is the huge gap in internet usage among South Africa on one hand, and the other countries on the other, which was obvious between 2000 and 2005, narrowed from 2006 through 2015, with the exception of Ghana. Generally, Figure 1 points to the increase in internet usage in Nigeria in the last eight years. This could largely be attributed to reduced internet cost, increased accessibility from mobile devices and expansion of e-commerce.

Table 1 displays information on secured internet servers in those countries overtime. Nigeria has the worst performance, with a value of 2.8 in 2016, compared to 6.3 in Ghana, and 124.5 and 10.7 in South Africa and Kenya, respectively. The intuition from this is that, despite the significant increase recorded in internet usage in Nigeria, a substantial proportion of the servers were not secured. This clearly explains the alarming rates of cybercrime in the country[2].

Table 1:Secure Internet Servers (Per 1 Million People) 2010-2016

	Secure Internet servers (per 1 million people)						
	2010	2011	2012	2013	2014	2015	2016
Nigeria	1.2044	1.68	1.757	1.693	2.334	2.616	2.8012
Ghana	1.713	2.189	2.914	2.581	3.671	4.966	6.275
South Africa	61.3	72.24	81.64	85.81	115.24	129.8	124.5
Kenya	2.53	3.1	4.12	4.72	7.6	8.91	10.77

Source: World Development Indicators (2016)

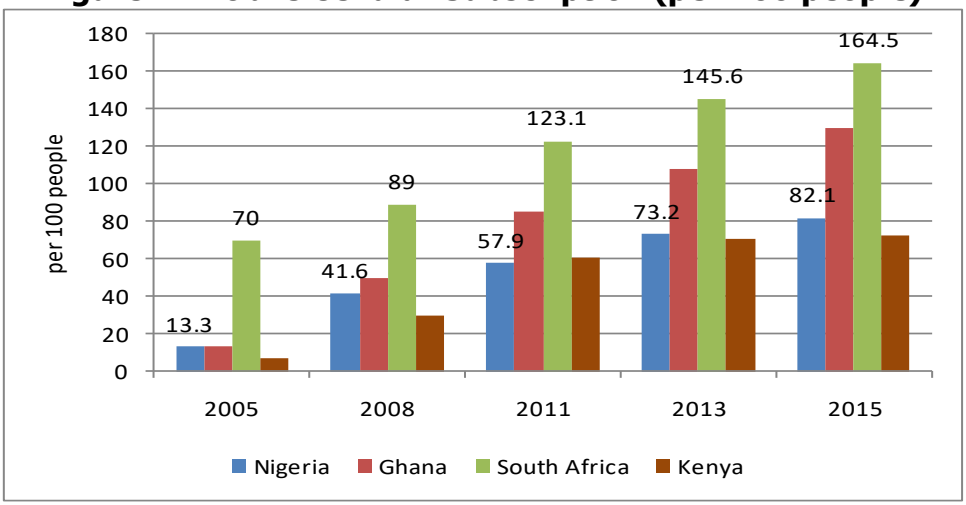
The trend of mobile cellular subscription in these countries is depicted in Figure 2. Mobile subscription in Nigeria increased substantially from 13.3 per 100 people in 2005 to 82.1 per 100 people in 2015. Nevertheless, when compared to South Africa and Ghana[3], which recorded 129.7 and 164.5, respectively in 2015, one would conclude

[2] Losses arising from cyber-related activities were estimated at ₦1 billion in 2016.

[3] These countries have smaller population sizes compared to Nigeria.

that much needs to be done in terms of remote connection in Nigeria.

Figure 2: Mobile Cellular Subscription (per 100 people)



Source: World Development Indicators (2016)

3.0 Conceptual Issues – Definition, Types and Dimension of Cyber Crime

3.1 What is Cybercrime?

Cybercrime is a topical issue that has been discussed by many people from various perspectives (Ibikunle and Eweniyi, 2013). One reason for this is the huge losses that were attributed to it. It was estimated that, global losses to cybercrime is about $400bn annually (CSIS, 2014). Others have put it at a higher value of $445bn[4]. As technology evolved, so did the definitions of cybercrime. According to Halder and Jaishankar (2011), cybercrime is an offence, with a criminal motive, committed against an individual or group of persons intentionally to harm the reputation of the victims as well as cause irreparable damage to hardware of sensitive infrastructure, including internet and mobile phones. Symantec Corporation, the world's biggest computer security company, defined cybercrime as any crime committed using a computer, network or hardware devices (Theohary and Finklea, 2015).

To explain what cybercrime means, let us look at the slit meaning of the words 'cyber' and 'crime'. The word 'cyber' has its origins from 'cybernetics', which refers to the science of communication that deals with the study of automatic control systems (much like the human nervous system/ workings of the brain) as well as the mechanical-electrical communication systems. Cyber is therefore a derivative of cybernetics used to describe interactions that relate to, or involve computers or networks. 'Crime' refers to the specific actions or inactions due to negligence that is injurious to public welfare or morals, and one that is legally prohibited. Cybercrime (e-crime or hi-tech crime) is a global phenomenon which takes place in the cyberspace i.e. in the world of computers and on the internet. Cybercrime involves using specialized applications in computers with the internet by technically skilled individuals to commit crime. The aftermath of such crimes may threaten a nation's security architecture and financial health (Saul, 2007). So, cybercrime can simply be explained

[4] See http://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

as a crime carried out with the aid of a computer system. It refers to criminal acts that are facilitated through the use of the internet.

3.2 Types and Dimension of Cybercrimes

In the past, little was known about cybercrime, but as the internet grew worldwide, the unintended consequences of computerization manifested in global notoriety. It is a worldwide problem that costs countries, businesses and individuals billions of dollars. The first reported cybercrime was committed by employees of a company in the 1960s and involved the company's mainframe computer (Maitanmi et al., 2013). In recent times however, it not only involves employees of companies or nations, but includes organized criminal gangs, terrorists, rogue governments and individuals (in isolated cases).

Lewis (2002), identified four important elements when assessing the risks of cyber crime. First, infrastructure as a target: cyber warfare and terrorism were placed in the historical context of attacks against infrastructure. Second, routine failure versus cyber attack: examining cyber attacks against a backdrop of routine infrastructure failures. Third, weapons of mass annoyance: the measurement of the dependence of infrastructure on computer networks and the redundancy already present in these systems. Finally, hacking and terror: for the case of cyber-terrorism, the use of cyber weapons in the context of the political goals and motivations of terrorists, and whether cyber-weapons are likely to achieve success.

According to Broadhurst (2006), computer crime encompasses criminal activities which can aptly be categorized by its unique typology of computer-related crime, comprising conventional crimes in which computers are instrumental to the offence. This is the case of child's pornography and intellectual property theft; attacks on computer networks; and conventional criminal cases in which abound undeniable evidence in digital form. The kinds of criminality include the following and is not limited by the underlisted issues:

i. Interference with lawful use of a computer: cyber vandalism and terrorism; denial of service; insertion of viruses, worms, ransomware and other malicious code.
ii. Dissemination of offensive materials: pornography/child pornography; on-line gaming/betting; racist content; treasonous or sacrilegious content.
iii. Threatening communications: extortion; cyber-stalking.
iv. Forgery/counterfeiting: ID theft; IP offences; software, CD, DVD piracy; copyright breaches et cetera.
v. Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual 'snake oils'); on-line securities fraud.
vi. Others include illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering.

Hassan et al. (2012), categorized cybercrimes into cyber terrorism, Cyber fraud, malware, cyber stalking, spam, wiretapping, logic bombs and password sniffing. Wada

and Odulaja (2012), included phishing and fake copy-cat websites to the types of existing cybercrimes. These are distinguished below.

(i)Cyber Terrorism - Lewis (2002), defines cyber-terrorism as the malicious act of using computer network to disrupt the normal processes of critical national infrastructures (such as energy, transportation, government operations), including the coercion or intimidation of public and private citizens. Hassan et al, (2012), described cyber extortion as a sort of cyber terrorism whereby the website, e-mail server, i or computer system leveraging on ransomware is put under attack by hackers for denial of services and demand for ransom.

(ii)Fraud (Identity Theft) - Fraud refers to the act of depriving a person dishonestly of something, which such an individual are supposedly entitled to possess. It verbally means an act of deception deliberately carried out to gain unlawful advantage. For fraud to be ascertained, there must be established, a case of dishonest intention to benefit (on the part of the perpetrator) at the detriment of other individual or organization (Eseoghene, 2010). The concept of Identity Theft is simple; someone gains access to someone's personal information and uses it for his/her own benefit.

(iii)Malware – "Malware", also known as malicious software, refers to the use of software or code designed to by-pass some security checks in computers/mobile devices and harness data without consent (MacAfee, Apr 23, 2013). Malicious logics include developmental faults such as Trojan horses, logic or timing bombs, trapdoors and zombies. It also includes operational faults such as viruses or worms (Avizienis et al, 2004). Powell and Stroud (2003) describes these faults as follows:

i. Trojan horse performs illegal action with the impression of being legitimate. This may involve the disclosure or modification of information which is essentially an attack against integrity and confidentiality.
ii. Logic bomb remains dormant in the host system until a certain time or an event occurs, or certain conditions are met, before it begins to delete files, slow down or crash the host system.
iii. Virus replicates itself and joins another programme when it is executed, thereby turning into a Trojan horse (a virus can carry a logic bomb). Worm replicates itself and propagates without the users being aware of it (a worm can also carry a logic bomb).
iv. Trapdoor provides a means of circumventing access control mechanisms.
v. Zombie can be triggered by an attacker in order to mount a coordinated attack.

(iv) Cyber Stalking – According to Ellison and Akdeniz (1998), cyber stalking refers to the use of the internet, e-mail, or other electronic devices to stalk another person. Cyber stalking can be used interchangeably with online abuse or online harassment. The perpetrator does not present a direct physical threat to a victim, but follows the victim's online activity, gathers information and eventually makes threats towards the victim.

(v)Spam – This refers to unsolicited bulk electronic mail (e-mail) and short message services (SMS) sent indiscriminately to prospective victims of crime via electronic

messaging systems. It is possibly the most practical cyber attack weapon because of its low operating cost (which ends with the maintenance of mailing lists) and the difficulty that would be associated with holding anyone accountable for mass mailings. The perpetrators, known as spammers, rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts.

(vi) Wiretapping/Illegal Interception of Telecommunication –
Telephone fraud has always been a problem. However, with an increase in the use of cellular phones as well as the ability to purchase goods and services with credit cards over phones, the problem has increased dramatically in recent years. Criminals use wiretapping methods to eavesdrop on communications and gain access to information which they should not be privy to.

(vii) Password Sniffing - Password sniffers are programmes which are designed to collect the first 128 or more bytes of network connections within a defined network being monitored (Hassan, et al, 2012). Crackers have them installed on networks used by systems that they intend to hack or penetrate. The sniffer collects information when users type in information such as usernames and passwords, usually required when using common internet services. Other programs sort through collected information, pull out important pieces such as the usernames and passwords, and cover up their existence in an automated way.
(viii)Phishing - High-tech identity theft that steals personal information and identity of unsuspecting users as well as commits acts of fraud against the legitimate individual or organization that have been victimized. The perpetrators send false emails fraudulently designed to mimic legitimate businesses, requesting for personal information which if released can allow them access one's bank accounts, including details of debit and credit cards.

(ix) Fake Web-Sites - There is the emergence of fake 'copy-cat' websites that take advantage of customers who are unfamiliar with internet usage or unsure of the real web site address of a legitimate company. Customers unwittingly enter their personal details into the fake web sites of criminals who either use the details themselves to commit crime or sell on the details to other interested fraudsters.

4.0 Causes and Effects of CyberCrime in Nigeria

4.1 Causes of CyberCrime

The root causes of cybercrimes are not far-fetched. One only has to take a quick glance around the society to observe illicit wealth acquisition and its display. This is coupled with the fact that, the perpetrators are highly exalted. The problem is made worse by the high youth unemployment, the absence of enforceable prohibitive laws and the general laissez faire attitude of individuals and businesses regarding cyber security (Hassan et al., 2012). Evidence has also shown that, a significant proportion of these crimes are perpetuated by people in their youthful age. It is however worth noting that some of these attacks are also perpetrated within organizations. Many internet users are easily lured by unknown mails and web site addresses, falling victim to spyware and phishing.

Hassan et al. (2012) identified urbanization, high unemployment, quest for wealth, poor implementation of cybercrime laws, inadequately equipped law enforcement agencies, and negative role models as some of the causes of proliferated cybercrimes in Nigeria. Akwara et al., (2013), in their study examined the relationships among unemployment, poverty and insecurity in Nigeria.

They found that unemployment causes poverty, and that a positive causal relationship exists between the latter and insecurity. Other causes of cybercrime according to them are: corruption, gullibility/greed, proliferation of cyber cafes and the vulnerable nature of the internet. The main causes of cyber-crimes in Nigeria are briefly discussed below.

(i) Urbanization – Rapid urbanization in Nigeria which manifests mainly through the fast population growth is a challenging issue for policy makers. Urban population grows at an annual rate of 4.3% (WDI, 2016). This is much higher than the Sub-Saharan Africa average and continues to put pressure on available resources in Nigerian cities. For instance, only 32.8% of urban population had access to improved sanitation facilities in 2015, and about 68.5% of urban population had access to potable water supply within the period (WDI, 2016). According to Meke (2012), urbanization is beneficial only to the extent of availability of good jobs that have been created in cities, amidst high population growth rate. The study held that urbanization is one of the major reason that led to increases in cybercrimes in Nigeria. He also noted that urbanization and crime move in tandem.

(ii)Unemployment – Unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. Youth unemployment rate is currently above 47%. According to Okafor (2011), high unemployment in Nigeria comes with socio-economic, political and psychological consequences. This phenomenon encourages the development of street youths and urban urchins ("area boys") that grow up in a culture that encourages criminal behavior.

(iii)Quest for wealth - Carnal instinct that quests for wealth is another cause of cyber crimes in Nigeria. For any business to succeed, it is expected that, the rate of returns on the investment grow at a geometric rate, with minimal risk. Cyber criminals desire to invest minimal capital in a conducive environment that would reap maximum gains as they strive to become rich using the quickest means possible.

(iv)Poor Implementation of Cybercrime Laws and Inadequately Equipped Law Enforcement Agencies – According to Laura (2011), African countries have received intense criticism for inadequately handling of cybercrimes due to inadequate infrastructure and competence of assigned law enforcement agencies. The private sector also lags behind in protecting itself from cyber savvy criminals, Nigeria inclusive. There is no sophisticated hardware to forensically track down cyber criminals. In some instances, the laws regarding cybercrimes are circumvented by criminals. It is worth noting that law enforcement agencies in Nigeria such as the EFCC and ICPC have successfully prosecuted cybercrime offenders over the years. Nevertheless, much improvement can still be made.

(v) Negative Role Models - Youths are mirrors of the society. According to Meke (2012), many parents transmit criminal tendencies to their children via socialization. If this continues unchecked and the values are absorbed by the younger generation, they will see nothing wrong with cybercrime.

(vi) Corruption – Nigeria has continued to occupy despicable position in the global ranking for corruption. In 2018, Nigeria was ranked the 144th most corrupt nation in the world out of 176 countries surveyed by the Transparency International[5]. People celebrate wealth without questioning the source of such wealth. It is common to hear of people with questionable character and wealth being celebrated in society. This misguided disposition towards wealth encourages the get-rich-quick mind set that can be pursued through cybercrime.

(vii)Gullibility/Greed – Most victims of cybercrime express some degree of gullibility and/or greed. Some people carry out transactions hoping to make profits without thorough investigations. Such people are preys for the cyber criminals.

(viii)Poverty - According to Jolaosho (1996), poverty refers to the inability to afford decent food, shelter, clothing and recreational activities. Hence, poverty is the absence of basic life essentials for survival and comfort of mankind. A poverty-stricken person may unwittingly turn to crime for survival. About 50% of Nigerians live in extreme poverty as at 2018.

(ix)The Proliferation of Cyber Cafes and the Porous Nature of the Internet - It is important to note that the nature of the internet is that geographical and political boundaries are not relevant as attacks can be generated by criminals from anywhere in the world and executed wherever the criminals deem fit. Also, the proliferation of cyber cafes has been another major cause of the rising cyber crime.

4.2 Effects of Cybercrime

Hassan et al. (2012) identified reduction in competitive edge of organizations, time wastage and slow financial growth, slow production time and increase in overhead cost, as well as defamation of the image of a nation as some effects of cybercrime. Other major effects include monetary losses and loss of privacy. Some of the effects of cybercrime are briefly explained below:

(i) Reduction in Competitive Edge- An organization can lose its competitive advantage and suffer losses when a hacker steals its confidential information and future plans and sells it to a competitor. The time spent by IT personnel on rectifying harmful incidents caused by computer criminals could have been used to earn profit for the organization.

(ii) Productivity Losses and Rising Cost- Cybercrime also reduces the productivity of an organization, as businesses take measures to prevent it by securing their

[5] See https://www.transparency.org/news/feature/corruption_perceptions_index_2016

networks. This is time consuming and also affects productivity. In addition, to control viruses and malware, organizations buy security softwares to reduce the chances of attacks. Computer crime therefore increases overhead cost and reduces profit margins. Other effects include the consumption of computer and network resources, and the cost in human time and attention of deleting unwanted messages.

(iii) Monetary Losses- The financial costs to economies and businesses from cyber-attacks include the loss of intellectual property, financial fraud, and damage to reputation, lower productivity, and third party liability. Opportunity cost (lost sales, lower productivity, etc) make up a proportion of the reported cost of cyber-attacks and viruses. However, opportunity costs do not translate directly into costs to the national economy. Businesses face greater damage from financial fraud and intellectual property theft over the Internet. Thus, where cybercrime is rife (especially relating to businesses and financial institutions) there are bound to be untold financial consequences. A research report by Ponemon Institute (2016) shows that, cybercrime cost in six countries (U.S.A, Japan, Germany, U.K, Brazil and Australia) in 2016 ranged from USD$4.3 million to USD$17.3 million annually. The study used a sample of 237 companies in the six countries.

(iv)Destroys Country's Image- One key negative effect of cybercrime is that it tarnishes a country's image. Once a country is labeled as a harbor for cybercrime activities, potential investors are cautious in investing in such countries. This has some dire implications for the nation's macroeconomic stability.

(v) Retards Financial Inclusion- proliferation of cybercrime in a particular country discourages financial inclusion, due to the fear of being a victim of cyber attack.

5.0 The Impact of CyberCrime on the Economy and Nigerian Banking System

Advancement in ICT no doubt brought with it, unlimited opportunities (particularly internet and financial softwares) for banking institutions in Nigeria. It facilitated ease of transactions and reduced cost for both depositors and the banking institutions. However, it also introduced its own peculiar risks through cybercrimes which have negatively impacted the industry and the economy in no small measure. The threats are enormous to citizens of any nation. Some of the impacts of cybercrime on the Nigerian economy are discussed below:

i. Cybercrime is no doubt providing a dent on Nigeria's image which remains a crucial source of national embarrassment for the country. The fear of cybercrime has made several persons to avoid the use of ICT. This has a negative impact on the welfare of the citizenry and investors. Confidence in a nation's financial system could be eroded by activities of cyber criminals. Potential investors and tourists are equally scared and the image of citizens is tainted.

ii. Citizens face reputational risk - in today's global economy, a nation cannot afford to have its reputation and that of its financial system tarnished by being associated with cybercrime. It becomes a problem for a citizen to engage in

meaningful social interaction with the rest of the world when every citizen is perceived as a potential scammer.

iii. The perceived loss of confidence may also affect the country's developmental progress, as foreign investments find it difficult to flow into the economy. This gives the nation an economic pariah status. The lack of confidence in the banking sector as a result of cybercrime can also be devastating on the economy.

iv. Impact on the financial Services Industry

It is well-known that a buoyant economy thrives on an effective and efficient financial system. Cyber-attacks are usually skewed toward deriving financial gains. Banks, other financial institutions, businesses and individuals bear the losses of such acts. Some economic impacts of cybercrime in Nigeria include:

a. Increases in the operating cost of businesses due to huge expenses incurred on purchase of security software applications to reduce the rate of cyber-attacks.
b. Failure of institutions arising from huge losses from cybercrimes - this could lead to a loss in confidence in the financial institutions and a possible run on them (where banks are involved), with possible contagion effects.
c. Increase in provisions - while loan loss provisions are predictable with some level of recoverability, losses arising from cybercrimes are not predictable; leading to increase in irrecoverable provisions and a consequent depletion of capital for banks and business entities. This could undermine confidence level in the nation's financial system.
d. Regulators and Supervisors of licensed deposit-taking institutions may be required to use taxpayers' money to resolve problems arising from cybercrimes. This may be in the form of problematic deposit-taking institutions receiving a lifeline through Prompt Corrective Actions or where institutions (banks) eventually fail, there would be the depletion on the Deposit Insurance Fund (DIF) to pay off depositors. Some of the modes through which cybercrimes are perpetrated in Nigeria include: theft/cloning of customer bank cards; fraudulent transfer or withdrawal of customer funds; hacking of banking software for the transfer of funds; cloning of bank/business websites to deceive customers and sending of emails/text messages requesting for personal information or assistance from unsuspecting individuals. Over the years, Automated Teller Machine (ATM) cards and Web Based (Internet Banking) frauds have contributed significantly to fraud cases in the Nigerian banking system. Table 2 shows the contribution of cybercrimes to total fraud loss in the Nigeria banking system between 2011 and 2016.

Table 2
Contribution of Cybercrime to Total Fraud Loss in the Nigerian Banking Industry (2011 - 2016)

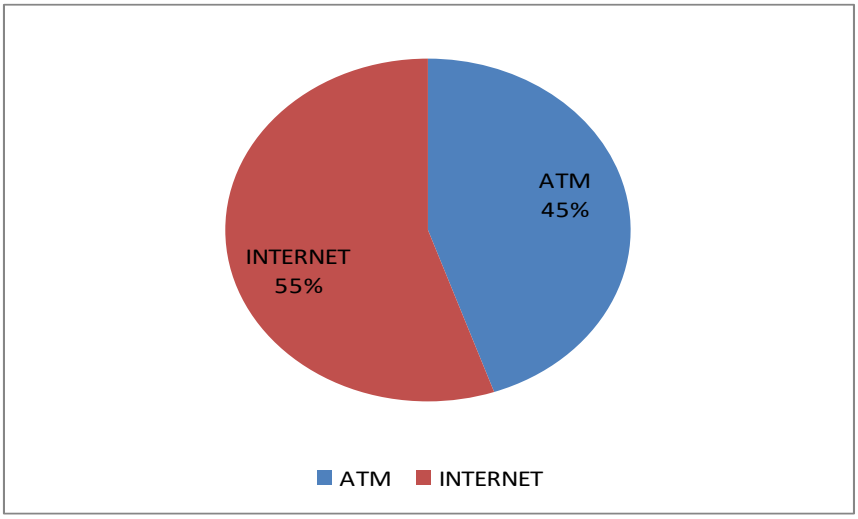
Year	Cybercrime losses(ATM & INTERNET) (₦ billion)	Growth rate of cybercrime losses (%) year-on- year	Total Fraud Loss (₦ billion)	Contribution Of Cyber Crimes To Total Fraud (%)
2011	0.115	-	4.071	2.82
2012	0.794	590.4	4.516	17.58
2013	2.268	185.6	5.757	39.40
2014	4.438	95.6	6.193	71.66
2015	1.361	-69.3	3.173	42.89
2016	1.058	-22.2	2.4459	43.26

Source: NDIC Annual Report (2011-2016)

The second column shows the actual losses from cybercrime over the years, while the third column depicts the year-on-year growth rate. Beginning from 2015, one can infer the gradual decline in losses from cybercrimes in Nigeria. It declined further in 2016 to 22.2%. That largely reflects the positive performance of agencies such as the EFCC in checking cybercrime. It is also suggestive of the effectiveness of the Nigerian Cybercrime Act, 2015. On the flip side, Table 2 shows that, in recent times, cybercrime losses contribute almost half of the total banking fraud losses reported. In 2011, it was only 2.8%. It increased significantly to 71.6% in 2014 and declined gradually to 43.2% in 2016. A major deduction from this is that, the cyber space is a key channel through which financial fraud is being perpetrated in the Nigerian banking industry. This therefore reiterates our earlier stance that increased efforts should be geared towards curbing this criminal activity.

Figure 3 disaggregates cybercrime in Nigeria by sources in 2016. The two main sources considered are Internet and Automated Teller Machines (ATMs). It is evident from the Figure that, internet constitutes the larger channel through which cybercrimes were perpetrated in banks in 2016.

Figure 3: Cybercrime Dissagregation in Nigeria (2016)



Source: NDIC Annual Report (2011-2016)

6.0 Strategies for Combating Cybercrime in the Nigerian Banking System

Cybercrime has grown rapidly in Nigeria following the introduction of modern telecommunication and broadband technologies. Nigeria was ranked 16th in cyber-attacks vulnerability in Africa in 2016 by Check Point (a cyber-security vendor). The prolific growth can be attributed to the availability of resources as well as the relative ease with which the perpetrators can acquire the skills for committing such crimes. Cyber-attacks will continue to rise as Nigeria becomes increasingly technology-driven, hence, the need for prompt corrective actions to prevent or mitigate them. Combating the threats of cybercrime and attendant reputational challenges has been high over the past decades. Despite the negative threats posed by cybercrimes to businesses, financial institutions, and the country, the advancement of cyber technologies has increased productivity levels and reduced cost of businesses. It is therefore imperative that certain measures are put in place to stem the growing menace. Such efforts would require inputs and active participation of all relevant stakeholders.

Cybercrime cannot be easily and completely eliminated, but can be minimized. To reduce cybercrime to a minimal level in Nigeria, there would be a need for an active collaborative effort between individuals, corporate organizations and the government.

6.1 Role of Individuals, Financial Institutions and Businesses

Fighting cybercrime is a huge task. This is because, as technology advances to combat cyber threats, criminals get sophisticated by coming up with novel ways of perpetrating their acts. Government and organizations globally have come up with laudable ways of addressing cyber related crimes, some of which are already being deployed within the shores of Nigeria. These include:

i. The use of robust firewalls to prevent attacks and filter malware or suspicious malicious codes.
ii. Consistent training of IT personnel to monitor and detect unusual traffic/intrusions within the deployed I.T infrastructure.
iii. The enactment of stringent laws and prosecution of individuals in breach of same.

iv. Deployment of secure user access interfaces to ensure that only authorized persons are given access to corporate networks.
v. Frequent updating and upgrading of software and applications to be in line with recent global best practice.
vi. There is the need for effective cooperation and collaboration among banking institutions. For example, when fraudsters use computers or other ICT infrastructure to transfer funds from an individual account, such funds are deposited or moved to an account in another financial institution. The institution involved should cooperate effectively when such fraudulent transfers are detected.
vii. Enhanced Public Awareness

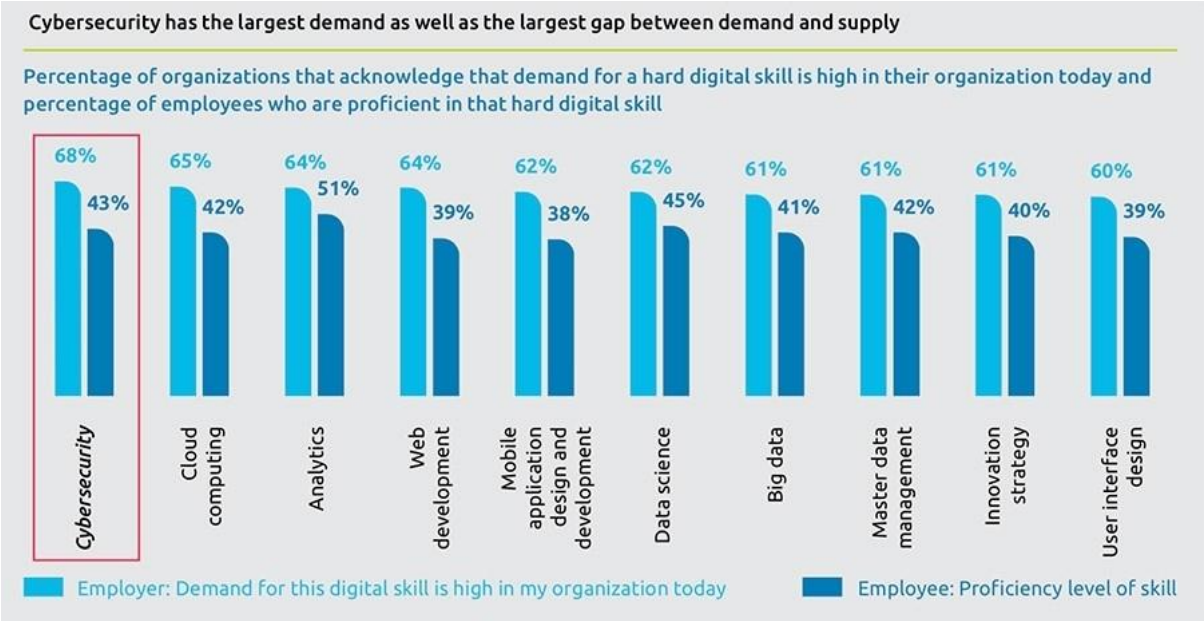
There is the need for adequate public awareness on the activities of fraudsters and consumer education on the usage of critical computer applications. Education is seen as the most vital weapon for literacy. There is the need for regular Seminars and Workshops to be organized from time to time with emphasis on cyber-safety so that individuals will learn to keep their personal information safe. There is the need for proper consumer education on the need to:

a. Observe simple rules such as ensuring the installation and usage of dedicated anti-malware protection/tool on each individuals computer systems, and avoid pirated software.
b. Personal Identification Number (PIN), bank account and email access should never be shared to unknown persons as systems are fraught with security issues. Irrespective of design and sophistication.
c. Confidential information should never be shared/ disclosed to anybody, as no network can 100% guarantee security from malicious hacking.
d. Ignore any unsolicited e-mail or SMS requiring any financial information.

Hassan et al. (2012) noted that, laws to enforce property rights work optimally when owners of property rights take reasonable steps to safeguard their property. Even with enabling laws and enforcement, institutions that operates wide network facilities, should take definite steps to secure their network, information and computer systems from malicious activities of cybercriminals. To achieve some success in reducing the level of cybercrimes in Nigeria, financial institutions and businesses should ensure the following:

a. Frequent user awareness and sensitization of end-users on need to ensure cyber security at all times.
b. Formulation and implementation of policies aimed at deploying and maintaining robust IT infrastructure on which the businesses thrive.
c. Subjection of deployed IT infrastructure to simulated attacks in order to ascertain vulnerabilities with the aim to address them i.e. Vulnerability Assessment and Penetration Testing.
d. The acquisition of insurance cover for losses relating to cybercrimes and attacks.
e. Create a forum for collaboration and sharing information on the nature, perceived origins and frequency of cyber-attacks experienced.

f. Organizing workshops for the purpose of building capacity for public and security operatives on proactive and sustainable ways of countering cyber-crime in Nigeria.



Culled from: Consultancy.uk

g. Enhancing operational risk management practices at all levels of the business. It is only logical for institutions to build resilient risk management frameworks that can surpass the sophistication of the cyber fraudsters.

h. Collaborative efforts of individuals, corporate organization and government would go a long way to reduce cyber crime to a minimal level.

i. Telecommunication Regulatory Agencies should ensure adherence to policies, procedures and standards that facilitate security on the internet service providers' infrastructure so as to easily detect and trace activities of cybercrimes. The enforcement on use of Security Incidence and Event Management (SIEM) will strengthen the process.

6.2 Role of Government

The CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015

As stated in its explanatory memorandum, the Cybercrimes Prohibition ACT 2015 "provides an effective, unified and comprehensive legal, regulatory and institutional Framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria". The Act needs to be constantly reviewed to align with dynamic nature of the cyber environment to accommodate more crimes and address more cyber-related issues that are unique.

The Nigeria Data Protection Regulation 2019 is also another regulation that is targeted at protecting both data in motion and at rest. Moreover, there are general laws that deal with financial crimes such as the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) Act 2004, and the Advance Fee Fraud and other Related Offences Act, 2006.

Okeshola and Adeta (2013) stated that for legislation on cybercrime to be relatively effective and efficient, government needs to empower graduates through employment and the provision of intensive training for law enforcement agencies on ICT to enable them in tracking down cyber criminals.

To reduce cybercrimes in Nigeria, there is the need to create job opportunities for the unemployed youths as well as the need for government, law enforcement, intelligence and security agencies to understand the technology and individuals engaged in the criminal acts in order to be able to curb their activities.

The social impact of cybercrimes is so damming that various tiers of governments have come up with different programmes aimed at re-orientating the youth towards positive thinking. Several initiatives directed at protecting the interests of Nigerians in the cyberspace have been put forward. Agencies, such as the National Information Technology Development Agency (NITDA), Nigerian Communication Commission (NCC), Economic and Financial Crimes Commission (EFCC) have all worked towards curbing the menace of cyber-crime in Nigeria. Other notable cyber crime control initiatives include the setting up of a National Cybercrime Working Group (NCWG) with stakeholders drawn from the law enforcement agencies, the financial sector and ICT professionals, and a pilot project of a Computer Emergency Response Team (CERT) centre by NCWG and NITDA. Cybercrime can however take place regardless of borders, but legislations and jurisdictions are based on a country-specific framework.

The upgrade of the Nigeria Financial Intelligence Unit (NFIU) to a full-fledged Agency (NFIA) is also a great leap to strengthen the fight against cybercrime in the country.

At the global stage, on the 12th November 2018, at the city of PARIS France, many countries came together and signed an accord for a secured and safe cyber space. The Paris call for trust and security in the global cyberspace is seen as a great achievement in the collaborative fight against cybercrime. The countries affirm their willingness to cooperate within the existing fora and through the relevant organizations and institutions to provide assistance, especially capacity development for less inclined nations. Notable amongst the areas of cooperation include:

i. Prevention and recovery from malicious cyber-activities with significant threat to individuals and critical infrastructure, and one that can lead to indiscriminate/ systemic harm;
ii. Check activities which substantially result in damages in availability or integrity of the internet for the majority of people;
iii. Strengthen the collective capacity of all members to easily detect and trace any misalignment/ interference by foreign actors, especially as it relates to malicious cyber-attacks of country's electoral processes;
iv. Put measure in place to stall theft of intellectual property garnered in ICT environment and this includes trade secrets and other confidential business information. The aim is to encourage competitive advantages amongst companies or commercial sector;
v. Competence should be enhanced in the areas of preventing the proliferation of malicious ICT tools and practices to stall its damaging effects;

vi. There are identified needs to strengthen the digital security and processes, as well as products/ services, throughout the supply chain lifecycle;
vii. Support efforts to strengthen an advanced cyber hygiene for all actors;
viii. Put measures in place that will check the activities of non-State actors, including the private sector, from conducting malicious hacking of systems, for own purposes or hired accomplices;
ix. Efforts should be geared towards promotion and implementation of acceptable international norms, as well as institution of measures to build confidence in cyberspace.

6.3 Role of NDIC

The NDIC, is one of the major stakeholders in the nation's financial system. As deposit insurer and a key component of the nation's financial safety-net, the NDIC has recognized the importance of effective management of all risks faced by the banking sector, including cybercrimes. Through the execution of its supervisory mandate of on-site and off-site supervision in conjunction with the Central Banks of Nigeria (CBN) and other members of the Financial Services Regulation Co-coordinating Committee (FSRCC), activities of all licensed deposit-taking financial institutions are reviewed regularly by the NDIC.

Banks in Nigeria are required by the provisions of Sections 35 and 36 of the NDIC Act No 16 of 2006 to submit monthly information/returns on frauds and forgeries to the NDIC. The mandate that financial institutions should put in place appropriate measures that protect their systems and customers against cybercrime is supervised and enforced by NDIC with vigour.

As part of the NDIC's efforts to protect depositors and combat infractions such as problems between customers and their bankers ranging from arbitrary interest charges, account balances manipulation to outright fraud & forgery as well as cybercrime issues, the NDIC introduced a 24-hour toll-free telephone line: 080063424257 to enable bank customers and the general public report any financial abuses for investigation and possible resolution. The NDIC also created a Complaints Unit in its Bank Examination Department and Special Insured Institutions Department (SIID) to address issues/concerns of bank customers. The NDIC encourages depositors and other stakeholders alike to avail themselves of the opportunity so as to assist it in its consumer protection efforts and promotion of public confidence in the financial system.

The recent attainment of the Three ISO Certifications in Information Security Management System ISO 27001:2013, IT Service Management ISO2000:2011 and ISO 22302:2012 Business Continuity Management BCM has highlighted the Corporations proactive measures against cybercrime. The Training of various staff on ISO 27032 (ISO Cyber Security), Certified Ethical Hacking (CEH) , Security Incident and Event Management (SIEM) as well as continuous Training and Education on Cyber Security within the Corporation has highlighted the Corporation's deepening of the cybercrime preparedness.

7.0 Conclusion

The rising spate of cybercrime globally and its attendant negative consequences has continued to call for immediate actions. As technology advances, novel methods are used to perpetrate cyber related crimes. Nigeria is not immune to these attacks, even though statistics show a decline in cybercrime losses in the country in recent times. That could be associated with the achievements recorded by fraud-prevention agencies such as the EFCC and other law enforcement agencies and provision of a legal framework for fighting cybercrime through the enactment of Nigerian Cybercrime Act 2015.

Nevertheless, it is expected that the cost of cybercrime may continue to increase as the convergence of IT and finance (FINTECH) becomes obvious globally and with the rise of crypto currency and the anonymity of transactions. There is therefore the need to take proactive steps to curb the menace.

Cybercrime poses a great risk to the economy, hence the need to institute an effective risk management system and enhancement of the capacity to carry out forensic investigation to tackle it. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cybercrimes.

Cyberspace is a challenging environment that is fast and continuously evolving. Hence, the challenge is for those charged with the responsibility of security in various quarters to be abreast of developments in the cyber world. The economic vitality and national security largely depend on a stable, safe and resilient cyberspace.

References

Akwara A.F., Akwara N.F, Enwuchola J., Adekunle M. and Udaw J.E. (2013): *Unemployment and Poverty: Implications for National Security and Good Governance in Nigeria*. International Journal of Public Administration and Management Research (IJPAMR), Vol. 2, no. 1.

Asemota, O.J, Ogujiuba, K, Aderemi, T.A and Mustapha, S (2015): *Modelling and Forecasting Teledensity using Univariate Time Series Models: Evidence from Nigeria*. International Journal of Statistics and Applications". Vol. 5(6), pp.279-287

Avizienis A., Laprie J. and Randell B. (2004): *Dependability and its threats: A taxonomy.* Article IFIP Advances in information and Communication Technology

Broadhurst R. (2006): *Developments in the global law enforcement of cyber-crime*, Policing: An International Journal of Police Strategies & Management, Vol. 29 Issue: 3, pp.408-433, Emerald Group Publishing Limited.

CSIS (2014) "Net Losses: Estimating the Global Cost of Cybercrime". Economic Impact of Cybercrime II. Center for Strategic and International Studies (CSIS), June 2014.

Ellison L. and Akdeniz Y. (1998): *Cyber stalking: the Regulation of Harassment on the Internet.* Criminal Law Review, Special Edition: Crime, Criminal Justice and the internet, pp 29-48.

Eseoghene J.I. (2010): *Bank frauds in Nigeria: Underlying Causes, Effects and Possible remedies*. African Journal of Accounting, Economics, Finance and Banking Research, 6(6): 62-79.

Esharenana E.A. and Stella E.I. (2008): *Combating cyber crime in Nigeria.*

Grabosky, P. and R. Broadhurst (2005): *The Future of Cyber-Crime in Asia'* Cyber-Crime: The Challenge in Asia, University of Hong Press.

Halder D. and Jaishankar K. (2011): *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global.

Hassan A. B., Lass F. D. and Makinde J. (2012): *Cyber crime in Nigeria: Causes, Effects and the Way Out*, ARPN Journal of Science and Technology, vol. 2(7), 626 – 631.

Ibikunle F. and Eweniyi O. (2013): *Approach to cyber security issues in Nigeria: Challenges and Solutions.* International Journal of Cognitive Research in Science Engineering and Education (IJCRSEE), Vol. 1, No. 1.

Jolaosho A.O. (1996): *Some Popular Perceptions of Poverty in Nigeria,* quoted in UNDP Human Development Report on Nigeria. Lagos: UNDP.

Justin Plot (2010): *Top five computer crime and how to protect yourself from them*, Publication of Justin plot.

Lakshmi P. and Ishwarya M. (2015): *Cyber Crime: Prevention & Detection*," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4(3).

Landwher C.E., Bull A.R., McDermott J.P.and Choi W.S. (1994): *A Taxonomy of Computer Program Security Flaws*. ACM Computing Surv., vol. 26, no. 3, pp. 211-254.

Laura A. (2011): *Cyber Crime and National Security: The Role of the Penal and Procedural Law.*

Lewis A.J. (2002): *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats:* Center for Strategic and International Studies, Washington, DC.

Maitanmi O., Ogunlere S. and Ayinde S. (2013): *Impact of Cyber Crimes on Nigerian Economy*, The International Journal of Engineering and Science (IJES, vol. 2(4), 45–51).

Meke E.S.N. (2012): *Urbanization and Cyber Crime in Nigeria: Causes and consequences*.

NBS (2012): Nigeria Poverty Profile, 2010. National Bureau of Statistics, Abuja

NDIC; Nigeria Deposit Insurance Corporation, *Annual Report* (Various issues).

Okafor E.E. (2011): "Youth Unemployment and Implications for Stability of Democracy in Nigeria", Journal of Sustainable Development in Africa Vol.13, No. 1.

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. Vol. 3, No. 9, pp 98-113.

Powell D. and Stroud R. (2003): *Conceptual Model and Architecture of MAFTIA*. MAFTIA.

Saul H. (2007): *Social network launches worldwide spam campaign* New York Times.

Theohary, C.A and Finklea, K (2015): Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement. Congressional Research Service Report.

Wada F. and Odulaja G.O. (2012): *Assessing Cyber Crime and its Impact on E-banking in Nigeria Using Social Theories.* African Journal of Computing & ICTs. Vol 5., No. 1, pp 69-82.

WDI (2016); World Development Indicator (WDI), International Bank for Reconstruction and Development/The World Bank; Washington D.C, USA.

https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf

https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/