Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.6, No.3, 2016

Interfacing ICT with Entrepreneurship Culture in a Developing Country in Contest with Cyber-Crimes: Gains and Pains

Chief Mrs. EZEANO, Victoria N
Chief Lecturer, Centre for Entrepreneurship Education (CEE.) Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State

Chief Dr. EZEANO, Nnaemeka A
Chief Lecturer Nze ii of Ele and Eze Mba-Ogu Kingdom Enugu-Agu Achi, Oji-River L.G.A, Enugu State, Nigeria

Dr. AMAH Peter
Department of Finance University of Lagos, Akoka

Dr. EZEANO, Caleb I.
Dept. of Agric. Economics & Extension Nnamdi Azikiwe University, Awka

Abstract
This paper is a cross-sectional analysis, critique and exposé of the impacts and the implications of the interfacing of ICT with entrepreneurship ventures in contest with cyber-crimes in a developing economy such as Nigeria. An entrepreneur is simply an individual who is willing to risk investing time and money in a business activity that has the potential to make a profit or incur loss. More specifically, the enterprising individual is someone who organizes production, bringing together the factors of production viz; land, labor, and capital to make goods and services. He makes business decisions, figuring out what goods to produce and how to produce them even in the face of the emerging cyber-crimes, knowing that there is no guarantee that business decisions will not be sabotaged. Again he innovates, introducing new products & technologies by the applications of information and communication technology (ICT) and related methods as new ways of organizing business. Entrepreneurs come from all types of background. The types of business they create come in all shapes and sizes. They range from, craft shops, wielding, foundries, rubber processing and vulcanizing, food eg "okpapreneur", ogiri-preneur, akpupreneur, palm-wine-preneur, compu-preneur etc. They are active in all classification of business activity, and are the foundation of the small business sector of our country's economy. Entrepreneurs are the proprietors of the apprenticeship system that provides primary vehicle for training the labor for small business. The apprenticeship system is one in which an individual serves a proprietor or master for a given period of time in order to learn a trade or craft. It generates a large multiplier effect in employment creation. Generally, there is also a reflection of gross under development of entrepreneurial culture in our academic curricula. Sorrowfully enough, the bane of our educational system curricula, inter alia, is that it is designed towards DEPENDABILITY instead of CREATIVITY to our students (FRCN Oral, 2015). Thus, the present curricula in use in our tertiary institutions should be reorganized and improved upon to serve as an engine of innovation, imagination and vision. The new curricula envisaged should expose students to courses which create opportunities for skill acquisition and entrepreneurship promotion, and broaden access to information and communication technology which encompass all computer-based systems such as tele-conferencing, video-conferencing and the Internet with its world wide web (www).The present picture of our educational system shows defects in national priorities due to lack of proper planning. Data from the National Universities commission show that, the Polytechnic and Colleges of Education enrolled relatively less number of students than the Universities. As a result, graduate output of Universities out-numbers that of other tertiary institutions designed to produce the middle level manpower. This clearly demonstrates that more managerial and executive personnel are produced than what is produced at the middle level, which otherwise should be more. Furthermore, Olaiya (1998) evaluated this problem of imbalance and posited that it has been reflecting in the poor performance of the economy. According to Ihekoronye (2000), the synthesis of this view and the lesson to be learnt from it is that a well planned manpower programme for the country ought to produce more at the middle level, bearing in mind that in an economy, where there are more managers and administrators than those producing and maintaining, there are resultant economic crisis, under-production, under-employment of high-level manpower, scarcity of necessary commodities and lack of appropriate technology development.
Keywords: Cyber-crimes, entrepreneurs, compupreneur, firewalls, computer forensics, ICT, "okpapreneur", palm-wine-preneur.

INTRODUCTION

The Internet has become a part of our daily lives as it is used for communication, research, networking, shopping, education, etc. With it, an individual (entrepreneur) can have access to a vast pool of information which will enable

participation in, negotiation with, controlling, and holding accountable; institutions that affect the individuals life. An entrepreneur is simply an individual who is willing to risk investing time and money in a business activity that has the potential to make a profit or incur loss. To achieve this, the entrepreneur organizes production, bringing together the factors of production viz; land, labor, and capital to make goods and services; in addition to making business decisions, figuring out what goods to produce and how to produce them. In other to add value to products/services, the entrepreneur innovates, introducing new products & technologies by the applications of information and communication technology (ICT) and related methods as new ways of organizing business. With this, he takes risks even against the emerging cyber-crimes, knowing that there is no guarantee that business decisions will not be sabotaged.

Again, entrepreneurs are the proprietors of the apprenticeship system (apprenticeship system is one in which an individual serves a proprietor or master for a given period of time in order to learn a trade or craft and it generates a large multiplier effect in employment creation). This system provides primary vehicle for training the labor for small business. They are active in all classifications of business activity, and also the foundation of small business sector of our country's economy. Arguing in support of this, Ezeano, Edmond, Isineyi, Urom, & Ikpe, (2011), asserted that there is every need to train up entrepreneurs (middle-level manpower) with appropriate qualities, characteristics and attitudes for a sustainable economic advantage, especially in this time when global economy is catalyzed by innovation.

A miracle of national transformation took place at the birth of the nation of Israel in 1948, courtesy of a providential breakfast meeting initiated by the Minister of Education at the home of the pioneer Prime Minister of the brand new fragile nation, Gen. Ben Gurion. The minister called on Ben Gurion early in the morning and shared with him his burden for their national survival and future. He put it like this *"you know we have been all along a trading people who have lived on law practice, buying and selling, managing money for themselves and others. In this our new state of Israel on a hostile Palestinian desert, there is not much to buy or whom to sell to. If we do not anything quick to change our lifestyle and means of living; with nothing to buy or sell, we shall soon start selling one another for survival. We MUST teach our people to start creating things with their hands i.e.* ENTERPRENEURSHIP EDUCATION**",** Nebo (2012). These two good heads put their thoughts to knock out vocational/entrepreneurial education that turned the deserts to Eden and consequently, Israel became the megastar and envy of all nations.

Why Become an Entrepreneur?

Individuals who venture out on their own into the market-place as entrepreneurs do so for a combination of three reasons:

1. The desire to control their own destinies. This desire brings about the greatest benefits and is often the greatest motivator. As small business owners, individuals control how they wish to run their personal lives. Entrepreneurs plan their own business activities and they schedule their professional responsibilities/duties around their personal priorities. This right is the greatest reward of entrepreneurship.
2. They desire to achieve freedom from direct supervision of a boss. Entrepreneurs still must answer to those on whom they depend, such as bankers, suppliers, or possibly transceiver; however these relationships are on equal basis and not a subordinate.
3. Desire to achieve greater profits: They strive for the potential to achieve profits greater than a salary earned from working for someone else. This is the hardest objective to achieve and usually takes the longest to accomplish. If the determination to succeed is present, it can be a reachable goal.

REVIEW OF LITERATURES AND DISCUSSIONS

It is a well known fact that "the Internet is the ultimate vehicle for information retrieval and transmission" (http://miter.mit.edu/articlesecurity-entrepreneurs-needed-cyber-crime-and-internet-security/), in this era of information superhighway age. Individuals from around the world are linked up in real-time, families, businesses and governments, connected. In spite of this vast expanse of digital data-flooding, otherwise known as the "cyberspace", attempts to decipher and exploit this information for personal or national gain have become increasingly pervasive. All information being stored and transmitted over the internet is vulnerable to attack. David, Karl, and William (2010) stressed that "four out of every five computer crimes (cyber-crime), investigated by the Federal Bureau of Investigation (FBI) in 1993 involved unauthorized access to computers via the Internet." In this age of connectivity, so many organizations have suffered from the activities of cyber-criminals.

Cyber crime, otherwise known as computer crime, e-crime, hi-tech crime or electronic crime is the use of computers to facilitate crime that is aimed at individuals/organizations, or at computers. This "crime is responsible for the economic losses that internet users have been facing lately" (http://www.spamlaws.com/fighting-cyber-crime.html). This can range from designing viruses, writing malware, cyber stalking, identity theft and various other crimes. Indeed, computer criminals do masquerade as authorized users and in the process, be able to figure out how to log-in and steal the business plans which an entrepreneur

may have labored over years, secret information about a product to be soon released or disclose a confidential material that may lead to loss of trade secret status; thus empowering a competitor to gain advantage of the market. Surely this will undermine the two cardinal goals of an entrepreneur/entrepreneurship --- i.e. creating wealth and employment opportunities.

Utomi (2003), posited that "entrepreneurship is the persistent pursuit of opportunity to create wealth through innovative creation of a product or service that meets the need of customers, using scarce resources in a way that results in the expectation of stakeholder whose roles sustain the business". With the use of the internet, in consulting others and exchanging of ideas among other things, the cost of production of goods/services will be greatly reduced.

Of a truth, Marcin Kleczynski (2012), revealed that small businesses, which are often the primary product of entrepreneurship and have an important role to play in any given economy; are increasingly the target for cyber criminals. To ensure the stability of an economy, the owners of these businesses need to understand the risks and take such measures to ensure that they are protected. To fight cybercrime there needs to be a tightening of national/international digital legislation and of cross-border law enforcement co-ordination. Interestingly, there is an important executive Bill before the Nigerian National Assembly called the "**Computer Security & Critical Information infrastructure Protection Bill" ("the Bill")**. This Bill would further assist the Nigerian National Assembly and the Nigerian people in having a better Law on wire-tapping, computer/cyber crimes, and anti-terrorism. The problem is the lack of operational law against cybercrimes in a country like Nigeria.

With the number of computer users worldwide increasing daily, as well as the different devices employed in accessing the Net, many users are becoming more complacent about the information they provide about themselves. The indiscriminate supply of personal information exposes a user to running the risk of allowing cybercriminals to gain an advantage (ITNOW, 2012). Computer usage is increasing, for both social and scientific areas, and it will continue to do so. This naturally leads to an increase in the ways in which individuals and the organizations' work may be attacked. In order to stay consistently ahead of a moving opponent, the criminals, organizations, and states that pose as a threat one needs to develop technical solutions, and improve one's capability in all areas of information security.

The introductory part of the Bill on "**new wire-tapping, cyber-crimes & anti-terrorism bill in Nigeria",** describes its objectives to include "… securing computer systems, networks and protecting critical information infrastructure in Nigeria by prohibiting certain undesirable computer-based activities…" This Bill seeks to create legal liability and responsibility for modern global crimes carried on a computer or over a computer-network, i.e. the internet. Some of these crimes carry penalties of fines ranging from the average sum of ₦100, 000.00 (One Hundred Thousand Naira) to terms of imprisonment ranging on the average, six months imprisonment, other cyber-crimes with penalties include:-

- Hacking and unlawful access to a computer or computer network.
- Spamming: This is the process by which unsolicited mails /fraudulent electronic mails, etc. are sent to different internet users.
- Computer fraud, computer forgery, and system interference.
- Identity theft and impersonation on the internet: This crime is becoming the order of the day because most internet users are not cautious with personal information such as National identity number, date-of-birth, credit card number, drivers license number etc. To avoid being a victim, one should always be careful with the provision of such information.
- Cyber-terrorism: This is described by this Bill to include any act which is a violation of the Nigerian Criminal Code or Penal Code, that endangers life, the physical integrity or freedom of any person or causes serious injury, death, loss or damage to public property, natural resources, the environment, cultural heritage, etc. Also, cyber-terrorism can be described as the use of computer, computer networks/internet to commit or promote terrorist crimes.. The penalty on conviction for acts of terrorism is a fine of not less than ₦10Million or a term of imprisonment for not less than 20 years or to both (Ehijeagbon, 2008).
- Cyber squatting: Cyber squatting is the assuming of the name, personality, trade or business name, trade mark, domain name or other names registered to or belonging to another person/local government/state/federal government in Nigeria. The penalty for breaching this provision on conviction is a fine of not less than ₦100, 000.00 (One Hundred Thousand Naira) or imprisonment of not less than one year or to both. (In Ezeano, et al 2012).

Because of the seriousness of cyber-crime, Section 3 of the said Bill makes it an offence for any person, without authority or in excess of such authority where it exists, to access any computer or access a computer for an unlawful purpose. Also, a disclosure of any password, access code or any other means of having access to any computer program without lawful authority is also inclusive. Section 12 of this Bill requires every service provider to keep a record of all traffic and subscriber information on their computer networks for such a period as the President of the Federal Republic of Nigeria may, by Federal Gazette, specify. Service Providers are further

required to record and retain any related content at the instance of any Law Enforcement Agency. This Bill also allows any Law Enforcement Agency in Nigeria, on the production of a warrant issued by a Court of competent jurisdiction, to request a service provider to release any information in respect of communications within its network, and the service provider must comply with the terms of the warrant. (ibid). This Bill seeks to ensure the protection of the privacy and civil liberties of persons by requiring that all communications released by a service provider shall only be used for legitimate purposes authorized by the affected individual or by a Court of competent jurisdiction or by other lawful authority. All law enforcement agencies carrying out their duties under this Bill must also have due regard to the constitutional rights to freedom of privacy guaranteed under the 1999 Nigerian Constitution and "… take appropriate technology and organizational measures to safeguard the confidentiality of the data retained, processed or retrieved for the purposes of law enforcement". To ensure compliance by the service providers or a corporate body, who are the providers of all form of telecommunication services in Nigeria, this Bill recommends that any breach of the provisions of the contemplated Law, by these persons, shall on conviction be liable to the payment of a fine of not less than ₦5Million. In addition, each Director Manager or Officer of the service provider shall be liable to a fine of not less than ₦500,000 or imprisonment for a term of not less than three years or both i.e. the fine and the term of imprisonments.

WIRE TAPPING AND UNLAWFUL INTERCEPTION OF COMMUNICATION

Wire tapping, which in modern parlance is known as Lawful Interception, described as the "… monitoring of telephone and internet conversations by a third person, often by convert means". It is unlawful, under the Bill, for any person to intercept any communication without the authority of the Owner of the communication. A conviction for a breach of this provision is a fine of not less than N5Million or imprisonment for a period of not less than ten years or to both the fine and the term of imprisonment.

It is mandatory under this Bill for all service providers to ensure that their networks are accessible and available to enable law enforcement agencies, on the production of an order of a Court of Law or of any other lawful authority, to intercept and monitor all communications on their networks, access call data or traffic, access the content of communications, monitor these communications uninterrupted from locations outside those of the Services providers, provided that these convert activities are for the purpose of law enforcement. The meaning of "…any other lawful authority …" is not defined in this Section or in the other Sections of the Bill neither is the responsibility of who bears the added technological costs of complying with these very stringent provisions indicated in the Bill. Any Service Provider that breaches the above provisions on cooperation with the law enforcement agencies would on conviction incur a fine of not less than ₦10million. As corporate bodies are artificial persons, additional liability is provided for each responsible Director, Manager or Officer of the Service Provider who allows any breach of the provisions of the Bill. A conviction of this group of individuals attracts a fine of not less than ₦500, 000 or imprisonment for a term of not less than three years or to both the fine and the terms of imprisonment.

Furthermore, some other assistance required of Service Providers and other relevant corporate bodies in prosecuting cyber-crimes include:-

- Identification, apprehension and prosecution of the offenders.
- Identification, tracing and confiscation of proceeds of any offence or property, equipment or device used in the commission of any cyber offence.
- Freezing, removal erasure or cancellation of the services of the offender from the network of the Service Provider.

The role of Internet access points in the facilitation of cyber crimes in Nigeria has been studied by Longe et al (2008). Their findings revealed that cyber cafes more than any other internet access points, have facilitated most cyber crimes. Indeed, of all the grand corruption perpetrated daily in our communities, most are of the agencies of computer and internet fraud , confirmed by (Onwudebelu, 2012) in (Ribadu ,2007)

SOME REAL LIFE EXAMPLES OF CYBER-CRIME

The Central Bank of Nigeria (CBN) in its banking sector supervision report revealed that the banking sector lost N7.2Billion (Vanguard, 2009) to Internet fraud in a year. Some customers have never recovered their money. Also, Shan Symington, a postman in Hampshire, UK, is yet to find those who stole £130,000 from him in MySpace, another networking website, in September 2007 by a Nigerian. Again, if Ola Bolawole, a graduate of Mechanical Engineering had examined a mail that came into his box requesting him to provide his personal account details for upgrading Automated Teller Machines (ATM), cautiously; he would not have been fleeced by internet fraudsters of his ₦800,000= lamented (Femi, 2010). The 419 scam letter ended with, "This email has been sent to all our bank customers and it is compulsory to follow, as failure to verify account details will lead to account suspension".

VICTIMS OF AUTOMATIC TELLER MACHINE

BANK CUSTOMER	GENDER	OCCUPATION	DEFRAUDED THROUGH	DEFRAUDED BY	AMOUNT (N)
1	M	Engineer	E-mail/ATM	Fraudster	800,000
2	F	Media practitioner	ATM	Unknown	40,000
3	M	Businessman	E-mail/ATM	Fraudster	350,000
4	M	-	ATM	Banker	490,000
5	F	-	ATM	Banker	10.8million
6	F	-	ATM	Unknown	133,000
7	M	Journalist	ATM	Unknown	40,000
8	F	-	ATM	Unknown	45,000
9	M	Businessman	ATM	Unknown	784,000
10	M	Planning officer	ATM	Unknown	30,000
11	F	Lecturer	ATM	Unknown	120,000
12	F	-	ATM	Family	50,000
13	M	Businessman	ATM	Banker	1million
14	M	Columnist	ATM	Banker	25,000
15	M	Student	ATM	Banker	6,000
16	M	System Analyst	ATM	Banker	5,000
17	F	Businessman	ATM	Fraudster	500,000

Sample output from a survey (Onwudebelu et al, 2012).

Cyber crime has become a career choice for an increasing number of highly educated young people who dismiss more conventional employment options (www.entrepreneurmag.co.za).

There are serious threats to these entrepreneurial aspirations and developments via cyber-crimes entrepreneurs guard and reinforce whatever cyber security measures that are available.

WHAT IS CYBER SECURITY?

It is a means of protecting ones personal digital information, and/or asset stored in the computer or in any digital memory device. There are different forms of threats and each one has its own levels of seriousness and solutions. The higher the degree of the terror, the more advanced or complicated the approach to enforce safety measures. The following are some of the reasons why cyber security is needed:-

- ✓ ***Hackers are everywhere:*** These could be a business rival, or neighbor, who has decided to take over another person's computer. Here software loopholes are capitalized on in hijacking another computer through backdoors, usually installed programs, or through cracking software. Having gained access to the target computer, all personal and confidential information (such as bank accounts, credit cards, or top trade secret, etc) can be employed in attacking other networks.
- ✓ ***Internet Scams and Frauds are Rampant:*** These include phishing, (a very organized cyber crime), which deceives people into giving their banking details. Cyber criminals, pretending to be representatives from legitimate financial institutions, send e–mail messages and ask unsuspecting people to verify their passwords, account numbers, and other vital information.
- ✓ ***Cyber Theft is a Common Cyber Crime:*** This is the most reported crime that has increasingly become an easy one used to steal information from computers, not only from individuals but for companies, banks, and other organizations as well. Though, hardly report, big companies lose large amounts of money.
- ✓ ***Virus infestation:-*** Virus reaches your system through a number of entryways. One is through unsecured and unknown websites from which you download files, programs, applications, or tools free of charge. Virus can slow down the system or even crash it.
- ✓ **Spyware:** This is a program that automatically installs itself on one's computer. It tracks personal information in one computer

CYBER SECURITY PANACEA

The National Computer Crimes Squad estimated that between 85 and 97 percent of computer intrusions are not even detected. Fewer than 10 percent of all computer crimes are reported (mainly because organizations frequently fear that their employees, clients, and stockholders will lose faith in them if they admit that their computers have been attacked), and few of the crimes that *are* reported are ever solved (David Icove, Karl Seger, and William VonStorch, 2010). Due to this ugly development, any internet user (entrepreneur) that wants to stay ahead of the game of cyber criminality and stay protected should apply the under-listed steps amongst others.

- ***Use Strong Passwords:*** Avoid using names, birthdays, addresses, and other personal information as

password. Do not use a word found in the dictionary as well, since hackers have found a way to decipher dictionary-generated passwords using certain tools. In general, a good password is at least eight-characters long and should be hard to crack. One can combine upper – and lower–case letters, numbers and symbols. Alternatively, one can use other methods to form a password that are unique and encrypted. This must be changed periodically.

- ***Regular updating of security Software:***
  Instalation and regular updating of security programs on one's computer is imperative so as to ensure that the business is protected against the latest emerging threats. Also, software such as web browsers, operating systems, adobe readers etc. need to be kept up to date.
- **Get anti-malware software:-**
  Malware or malicious software is a term used for a number of different types of programs designed to break into or damage one's computer (www.entrepreneurmag.co.za). Malware include; Viruses, Worms, Trojans, Spyware, etc.
- **Avoid Opening Files sent through Instant Messenger:**
- **Ignore the Links on Pop-up Windows:** Block pop-up ads and windows to close an entryway for malware and other forms of attack.
- **Avoid Downloading Files, Programs, Applications, or Tools from Unknown Websites**
- **Make Sure to keep your System Clean:** Remove any tool, application, or program that is not in use.

FINDINGS

In today's age, when everything from small gadgets to nuclear plants is being operated through computers, cyber-crime has assumed threatening ramifications. Indeed, the figures1&2, below – taken from the Internet Crime Complaint Center (IC3), highlight that the number of identity theft, stolen credit-card fraud and online scams have drastically increased over the past decade.

Figure 1: Yearly Comparison of Complaints Received via the IC3 Web site

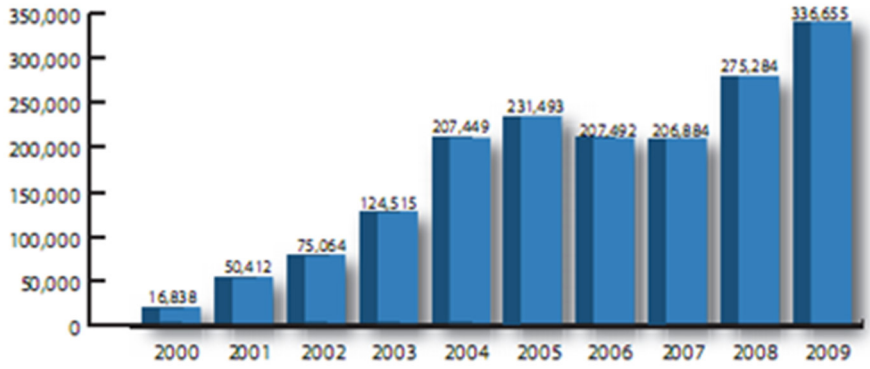
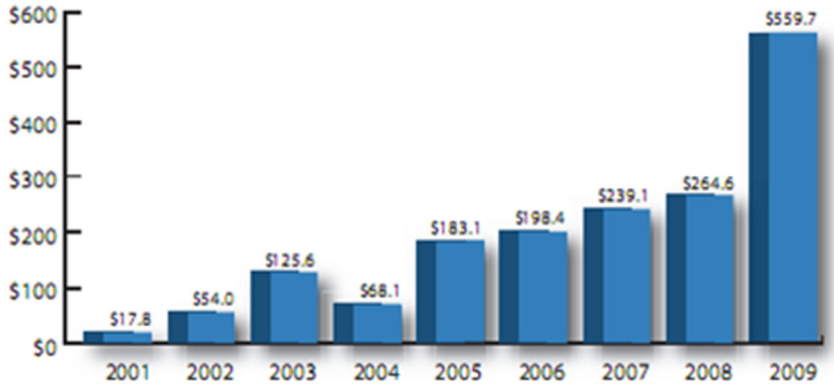


Figure 2: Yearly Dollar Loss (in millions) of Referred Complaints



http://miter.mit.edu/articlesecurity-entrepreneurs-needed-cyber-crime-and-internet-security/

Chuck McCutcheon (2005) alerted that there is an urgent need to educate non-computer professionals (entrepreneurs) on computer security. This will evidently curtail the huge financial and social burdens associated with cyber-crime even as these entrepreneurs join other information technology workers in protecting themselves

online.

The Nigerian government is not left out in this fight against cyber crime. This has led to the establishment of a cybercrime working group called the Nigerian Cyber Working Group (**NCWG**). The NCWG is an inter-agency body made up of all key law enforcement, security, intelligence and ICT agencies of government, plus major private organizations in the ICT sector. The group has agencies like the Economic & Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), the Nigeria Communications Commission (NCC), Department of State Services (DSS), National intelligence Agency (NIA), Nigerian Computer Society (NCS), Nigeria Internet Group (NIG), Internet Services providers' Association of Nigeria (ISPAN), National Information Technology Development Agency (NITDA), etc saddled with the task of eradicating the scourge from the nation, (Onwudebelu et al, 2012).

SUMMARY/CONCLUSION

Cyber criminals are relentless, highly organized, slick, and extremely manipulative in using more sophisticated methods to extract and abuse sensitive data. Since the internet has come to stay, and Cyberspace is at best lawless; only the one who understands/applies the relevant steps of self-protection survives. Although Cyber security professionals and police are in a depressing number, and the field being a relatively new area of information technology (recently pushed over the top by the increasing number of internet frauds and scams, cyber thefts, system crash, and other forms of cyber attacks); that should not make any entrepreneur to throw in the trowel. It is encouraging to note that the Federal Government has approved 1% of the Federation Account for National Agency for Science and Engineering Infrastructure's (NASENI) activities. Soon, therefore, Nigeria should have enough funds to carry out work relating to its national needs in the area of entrepreneurial developments even in our developing country, in order to fast-track the nation's **vision 20:2020**, if the legislation against cyber-crime is implemented .

LIST OF REFERENCES

Aaron Phillip, David Cowen, Chris Davis (2009). Hacking Exposed: Computer Forensics. McGraw Hill Professional. pp. 544. ISBN 0-07-162677-8.

Ashenhurst, Robert L (1986).Letter: ACM Forum, Communications of ACM,29(7): 586-592. AYasinsac, RF Erabacher, DG Marks, MM Pollitt (2003). "Computer forensics education". IEEE Security & Privacy.

David Icove, Karl Seger, and William VonStorch (2010). Fighting Computer Crime Computer Crime Research Centre (CCRC)

Chuck ,McCutcheon (2005). Viruses, hackers and other cyber security dangers. newhousenews.com

Dunbar, B (January 2001). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment".

Ehijeagbon ,Ohicheoya Oserogho (2008). New Wire Tapping, Cyber-crimes & Anti- terrorism Bill in Nigeria, PersonalFinance, page6

EXP-SA, Prediction and Detection of Network Membership through Automated Hard Drive Analysis". http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=0730389 20/04/2014.

Ezeano, V.N., Edmond, E. E., Isineyi, T. N., Urom, E. O., and Ikpe, D. N., (2011), Entrepreneurship: A Fundermental Approach. John Jacob's Classic Publishers Ltd., Enugu.

Ezeano, V.N (2012). Tackling the challenges of cyber crimes for National security, News commentary broadcast from FRCN Enugu Zonal station 16/07/2012.

Femi ,Ayodele (2010). Automated Theft Machine, The NEWS magazine,34(3):39-40

FRCN (Oral, 2015). Federal Radio Corporation of Nigeria discussion segment, Politics Nationwide , 20th May

Gordon, L. A, Loeb, M. Lucyshyn, W. and Richardson, R. (2005). CSI/FBI Computer crime and security, Computer security Institution:1-24

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1.951&rep=rep1&type=pdf 12/05/2014

http://books.google.co.uk/books?id-yMdNrgSBUq0C. Retrieved 27 August 2010.

http://www.sans.org/reading_room/whitepapers/covet/detailed-steganographic-techniques-open-systems-environment_677 23/05/2014

Ihekoronye, A.I.(1993). Technological Issues and Strategies for the Develppment of Small to Medium Scale Food Processing Industries in Papua New Guinea. In Employent, Agriculture and Industrialization. J. Millet (ed) INA/NRI Joint Publication 60:278-303.

ITNOW (2009). Careers, Making the grade**,** BCS London, July, pp.10-12.

ITNOW (2009). BOOST Your IT skills, BCS London, November, Pp.5.

ITNOW (2012). What's your SECURITY STRATEGY? British computer society,bcs.org/itnow, page18

Leigland, R (September 2004). "A formalization of Digital Forensics".

http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B8472C-D1D2-8F98-8F7597844CF74DF8.pdf 24/06/2014.

Longe, O. B and Chiemeke, S.C (2008). Cyber crime and criminality in Nigeria what roles are Interest access points playing, European Journal of Social Sciences, 6(4):132-139.

Marcin Kleczynski (2012). Fighting Cyber-crime: How to avoid malware and other computer viruses. www.malwarebytes.org.

Nduka, Okafor (1993). Biotechnology and Nigeria,s Economic Development, a Convocation Lecture at the Federal Polytechnic Unwana, Ebonyi State, 12th March.

Nebo, Ositadimma C.,(2012). The Imperatives of Engineering and Technical Vocational Education in National Development, 12th Convocation Lecture, Akanu Ibiam Federal Polytechnic Unwana

Olaiya, S.A. (1988). Training for Industrial Development in Nigeria, Ehindero (Nigeria) Ltd, Jos.

Onwudebelu,U and Alaba, O (2012). Determining the proper response to cyber crimes in Nigeria, Book of Proceedings 1st & 2nd Annual state conference , Nigeria Computer Society, Kogi State Chapter.

Ribadu ,Nuhu (2007). cybercrime and commercial fraud: a Nigeria perspective, modern law for Global commerce: congress to celebrate the fortieth annual session UNCITRA Vienna, 9-12 July.

Tucker, A.F, Deek, et al (2002). A model curriculum for k-12 computer science report of the ACM k-12 Education Task force computer science committee, ACM.

Vanguard (2009). Nigeria: cybercrime can wipe out developing gains of Nation experts. www.bio.org/node/517.

web.worldbank.org

www.biography.com/.../charles Babbage retrieved 25/01/15.