©IDOSR Publication
International Digital Organization for Scientific Research ISSN: 2550-7974
IDOSR JOURNAL OF ARTS AND MANAGEMENT 4(2): 87-97, 2019.

Effect of Cybercrime on Performance of e-business in konga.com.

Kenneth C. Nwekpa[1], Bernadine O. Ezezue,[2] Chikelue C. Nwabuike[3]and Patricia N. Ibeme [4]

[1-2]Department of Business Management and Entrepreneurship Studies, Ebonyi State University, Abakaliki, Nigeria, [3]Department of Management, University of Nigeria. and [4]Faculty of Management Sciences, National Open University of Nigeria
Correspondence email: chukwumake@gmail.com

ABSTRACT

The paper is on effect of cybercrime on performance of e-business in konga.com. Cybercrime has grown more prevalent, and consumer confidence has plummeted. Some studies reveal the prevalence of cybercrime; 65% of internet users globally have fallen victims to cybercrimes, including computer viruses, online credit card fraud and identity theft. The objective is to ascertain the degree of relationship between malicious agents on performance of e-business in Konga.com. The study took an ex-post facto survey design approach. Ex- post facto design was used because of the Time serial nature of the research. This study was carried out in Konga.com Abakaliki service point in Ebonyi State Nigeria. Pearson product moment correlation coefficient analysis and t-statistics were used to test the hypotheses raised. It was concluded that malicious agents are one of the strong inhibitors for e-business performance and are serious threats to the growth of e-business activities. It was recommended that e-business platforms should also consider the latest Biometric technology to data and information security against the regular password and code encryption amongst other.

Keywords: Cybercrime, Malicious agents, e-business and identity theft.

INTRODUCTION

Computer usage in everyday life and in business is on the rise [1]. E-mail, the Internet, and numerous other computer programs allow small businesses to focus on the conduct of their business, rather than on recordkeeping and communication processes.

e-business can be said to be the transaction of business activities with computers and computer networks. e-business is an imperative paradigm of business in the contemporary business world, geared at enhancing productivity, human resource management and customer services. [2] asserted that in order to participate in the new online business environment, businesses have had to make significant financial investments in necessary technologies, in processes and people necessary to operate them. And they further stated that to evaluate e-business investments or monitoring the resulting online business operations requires the existence of an appropriate performance measurement system.

However, with the growth of e-business is cybercrime also known as online crime. [3] defined Cybercrime as criminal activities which computers or computer networks are tools, and targets. Some of the major impacts of cyber-crime include; socio-political impacts, private and public sector businesses, consumer behaviour impact, emotional impact, lost of sales, cost of security protection and many more. Cybercrime has grown more prevalent, and consumer confidence has plummeted. A study by [4] reveals the prevalence of cybercrime; 65% of internet users globally have fallen victims to cybercrimes, including computer viruses, online credit card fraud and identity theft. And that cybercrime has now surpassed illegal drug trafficking as a criminal money maker. Someone's identity is stolen every three seconds as a result of cyber-crime, without a sophisticated security package, an unprotected PC can become infected within four minutes of connecting to the internet.

Konga.com is one of Nigeria's largest online marketplace. Konga.com started operations in July 2012 with a basic mission to become the engine of e-commerce and trade in Africa. It offers a third party online marketplace, as well as first party direct retail.

Konga.com offers products that span various categories of products including; Phones, computers, clothing, shoes, home appliances, books, health care, baby products, personal care and more. The services of Konga.com include lowest price guarantee, free return policy, order delivery- tracking, dedicated customer service support and many other premium services. Konga.com was founded by SimShagaya with about 20 staff at a start, and officially launched its third party retail platform in the first half of 2014, and acquired the assets and mobile license of Zinternet Nigeria Limited in june 2015, thereby meeting the central bank of Nigeria's legal requirement for the provision of mobile payment services.

Malicious agents on the internet are computer programs that operate on behalf of potential intruders to aid in attacking the system or network. This includes; computer viruses, spying agents, phishing, and remotely controlled agents. Frequent attacks of these agents on user instances could discourage registered users from visiting the Konga.com site (low visitation frequency). The objective is to ascertain the degree of relationship between malicious agents on performance of e-business in Konga.com.

LITERATURE REVIEW

Cyber Crime

[5] asserted that cybercrime is any illegal behaviour committed by means of or in relation to a computer system or network, which includes illegal possession and offering or distributing information by means of a computer system or network. [6] went further to list three major categories of cybercrime, which are all activities done with criminal intent in cyber space as, crimes against persons, crimes against business and non-business organizations and crimes against the government

They also outlined some examples of cybercrimes to include spamming, identify theft, hacking, phishing, denial of service, advanced fee fraud 419 (aka yahoo-yahoo) ,credit card fraud, software piracy, plagiarism, pornography etc.

[7] opined that cybercrime is used to broadly describe criminal activities in which computers or computer networks are tools, targets or a place of criminal activity and include everything from electronic cracking to denial of service attacks. They further categorized cybercrime as: Data crime (that is data interception, data modification and Data theft), Network crime (network interferences and Network sabotage), access crime (unauthorized access and virus dissemination) and related crimes (computer related forgery and content related crime). [8] gave the following types of cybercrime:-

a. Theft of telecommunications services.
b. Dissemination of offensive materials.
c. Electronic money laundering and tax evasion.
d. Electronic vandalism, terrorism and extortion.
e. Sales and investment fraud.
f. Illegal interception of telecommunications.
g. Electronic funds transfer fraud.

They further enumerated some impacts of cyber crime to include

a. Crime as an evil factor of society
b. Impact of cyber crime over socio- eco-political riders
c. Impact of cyber crime over teenager
d. Impact of cyber crime over private industry
e. Impact of cyber crime over consumer behavior
f. Emotional impact of cyber crime
g. Impact of cyber crime over business
h. Cost of security or protection
i. Lost sales
j. Impact of cyber crime over youth
k. Cyber bullying and (l)Sexual solicitation

[9] defined cyber crime as an act committed or omitted in violation of law forbidding or commanding it and for which punishment is imposed upon conviction. [10] mentioned some kinds of cyber crime to include :-

a. Crackers: individuals with intent on causing loss to satisfy some motives or just for fun.

b. Hackers: individuals that explore others computer systems out of curiosity with an attempt to gain acceptance as an expert without formal education.
c. Pranksters: individuals that perpetrate tricks on others with no intent of any particular long-lasting harm.
d. Career criminals: individuals that earn part or all of their income from crime
e. Cyber terrorists: individual that use the cyber to exhibit terrorism either by breaking into a public website or crashing a website
f. Cyber bull: individuals that harass others via the internet
g. Salami attackers: financial related crimes e.g a bank employee inserts a programme into bank's servers, which deducts a small amount form the account of every customer.

[11] opined that cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to identically harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones. [12] itemized some of the effects of cybercrime to include:-

a. Reduction of competitive edge of organizations
b. Time wastage and slow financial growth
c. Slow production time and more over head cost
d. Defamation of organizational image

[13] opined that cybercrime means a crime committed by an act or omission in the violation of law forbidding or commanding it and for which punishment is imposed on conviction. He gave some kind of cyber criminals to include :-

a. Crackers: Criminals having intention for causing loss to the victim to satisfy some anti social motives or just for fun
b. Hackers: Criminal who enter into the computer system or data base of victim to get the personal information hidden in those computer systems.
c. Pranksters: This criminals perpetrate tricks on others not intending any particular or long lasting harm.
d. Career criminals: This criminals adopts cyber crime as their career and earn part or all of their income from crime. In some cases, they conspire with others or work within organised gangs like the mafia.
e. Cyber terrorists: They attack on websites, mail accounts, phone books and others by sending malware, like viruses, Trojans, worms and the like to victims so that their database gets disturbed.their aim is to weaken the information technology infrastructure of the country so that they become unreliable for the forging investors and individuals who wish to become part of such victim country's IT system.
f. Cyber bulls: They harass victims through the internet. They send defamatory mails, posts which are vicious and making such a statement through the internet which causes harassment in any form to the victim.
g. Salami attackers: They attack through internet for the commission of financial crimes. The main intention is to make a little alteration in a single case which become unnoticed generally. for example a bank employee inserts a program into bank's servers which deducts a small amount from the account of every customer, such act is generally unnoticed, but the overall gain by the criminal is resulted into a huge loss to the victims.

[14] gave some impacts of cyber crime as:-

a. Potential Economic Impact: Involvement of losses in millions of dollars per year.
b. Impact on market value: The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies that provide cyber risk policies. Also accounting based measures like return on investment (ROI) are limited by the lack of time and resources necessary to conduct an accurate assessment of financial loss.

c. Impact on Consumer Trust: Cyber crime makes the loss of confidence in the customer and in the internet and its strengths. Also any concern over the credibility of an E-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. The slightest perception of security risk on e-business seriously paralyze the potential of business.

d. Effect on National security; information warfare, including network attack, exploitation, and defence on military systems are national security challenges. Owing to advance technology, such crimes can be committed from any part of the world and therefore criminals find loopholes in the security system of the victim countries.

Table 1; cyber crime type statistic 2015

Crime Type	Victim Count
N on-Payment/No n-Delivery	67,375
4 19/Overpayment	30,855
Identity Theft	21,949
Auction	21,510
Other	19,963
Personal Data Breach	19,632
Employment	18,758
Extortion	17,804
Credit Card Fraud	17,172
Phishing/Vishing/Smishing/Pharming	16,594
Advanced Fee	16,445
Harassment/Threats of Violence	14,812
Confidence Fraud/Romance	12,509
No Lead Value	12,187
Government Impersonation	11,832
Real Estate/Rental	11,562
Business Email Compromise	7,837
Misrepresentation	5,458
Lottery/Sweepstakes	5,324
Malware/Scareware	3,294
Corporate Data Breach	2,499
Ransomware	2,453
IPR/Copyright and Counterfeit	1,931
Investment	1,806
Crimes Against Children	1,348
Civil Matter	1,148
Re-shipping	1,073
Denial of Service	1,020
Virus	971
Health Care Related	465
Charity	411
Terrorism	361
Hacktivist	211
Gambling	131
Criminal Forums	62

Source; Internet crime complaint center 2016. pp 15

Table 2; cyber crime type losses 2015

Crime Type	Loss Amount(USD $)
Business Email Compromise	246,226,016
Confidence Fraud/Romance	203,390,531
Non-Payment/Non-Delivery	121,329,122
Investment	119,177,899
Identity Theft	57,294,589
Other	56,153,977
Advanced Fee	50,721,226
419/Overpayment	49,217,119
Personal Data Breach	43,477,526
Credit Card Fraud	41,503,502
Real Estate/Rental	41,417,647
Corporate Data Breach	38,800,430
Employment	33,890,824
Lottery/Sweepstakes	19,365,223
Auction	18,906,416
Misrepresentation	17,974,014
Extortion	14,799,705
Harassment/Threats of Violence	13,126,123
Government Impersonation	12,090,159
Civil Matter	9,946,345
Phishing/Vishing/Smishing/Pharming	8,174,316
1 PR/Copy right and Counterfeit	7,230,803
Re-shipping	3,831,957
MaIware/Scareware	2,912,628
Denial of Service	2,770,978
Ransomware	1,620,814
Charity	1,328,153
Virus	1,230,812

Gambling	955,360
Health Care Related	906,343
Hacktivist	171,601
Crimes Against Children	97,584
Terrorism	65,789
Criminal Forums	55,996
No Lead Value	0

Source:Internet crime complaint center 2016. pp 16

Table 1 above shows the various types of cyber crimes reported and recorded internationally in 2015. Non-payment/non-delivery crime accounted for the highest reported crime with victim count of 67, 375. However, E-mail scams also known as business E-mail compromise has 7, 837 victim counts with the highest loss amount of $246, 226, 016. Malicious agents also known as malware/scare ware has 3, 294 victim counts and $2, 912, 628 loss amount. While identity theft has 21, 949 victim counts and $57, 294, 589 loss amount.

Table 3 ;Top five countries by victim location

	Country	Percentage %
1	United states	80.2
2	United kingdom	2.47
3	Nigerian	2.2
4	China	1.91
5	India	1.46

Source: Internet crime complaint center 2016. pp 14

Table 3 above shows the percentage victim locations of cyber crimes in 2015. 80.2% of the victims were in the United States of America, 2.47% of the victims were in the United Kingdom, 2.2% of the victims were in Nigeria, 1.91% of the victims in China and 1.46% of the victims were in India.

Malicious Agents

[5] opined that malicious agents also called Black viruses are harmful processes which destroy any agent arriving at the network site where they reside when this occurs, malicious agents move, spreading to all the neighboring sites, thus increasing its presence in the network.

[9] asserted that Hypertext transfer protocol (http) has become the main protocol to carry out malicious activities. Attackers typically use http for communication with command and control servers click fraud, phishing and other malicious activities, as they can easily hide among the large amount of benign http traffic.

[13] gave suggestive measures to be taken against cyber-crime as:-

a. Avoiding disclosing any personal information to strangers via E-mail or while chatting
b. Avoiding sending any photograph to strangers by online.
c. Updating anti-virus software to guard against virus attack by users and also effective backup in order not to suffer data loss in case of virus contamination.
d. Not sending credit card number to any site that is not secured, to guard against frauds.
e. Parental control on sites to avoid harassment or depravation in children
f. Website owners to check irregularities on site.

g. As cyber crime is the major threat to all countries, steps to be taken internationally for preventing cyber crime.
h. Complete justice to be provided to victims of cyber crimes
i. Good and robust E-security or internet security systems to avoid corruption of files or enable criminal to access personal and financial information.
j. Investment in high tech softwares, antivirus, antispyware and antimalware
k. Firewall system which is used by all the operation systems, should be updated time to time
l. Data encryption techniques must be used during data transmission.
m. Use of voice recognizer, filter software and caller ID for protection against unauthorized access should be done.
n. Development of cyber forensics and biometric techniques.
o. Spam blocker to be turned on with internet providers.

[2] identified two models of firms performance as Economic model and organizational model. The Economic model emphasizes on the importance of external market factors in determining firm success. Whereas the organizational model builds on the behavioral and sociological paradigm, and sees organizational factors and there fit with the environment as the major determinants of success.

They further decomposed the Economic model to include:

a. Industry variables (characteristic of the industry in which the firm competes)
b. Variable relating the firm to its competitors
c. Firm variables (the quality and quantity of the firm's resources)

The organizational model in broad term suggests that managers can influence the behavior of their employees (and thus the performance of the organization) by taking into account factors such as the formal and informal structure, the planning, reward, control and information systems, their skills and personalities, and the relation of these to the environment. That is, managers influence organizational outcomes by establishing context, and the context is the result of a complex set of psychological, sociological and physical interaction.

[3] later integrated the two models of firm performance and their result confirmed the importance and independence of both sets of factors in explaining performances. [5] confirmed that E-business adoption has significant impact on service operations, cost operation reductions and profit levels (performance indicators) they further recommended more effective information technology (IT) training in order to further enhance the performance of E-business. And also that E-business managers should endeavor to procure quality IT gadgets that will enhance efficiency and customers retention.

[9] opined that E-business offers buyers and seller a new form of communication and provides an opportunity to create new marketplace. They further stated that E-business has positive effects on performance of e-business in large firms mostly.

New growth theory (Endogenous growth theory)

[14] is credited with stimulating new growth theory. The theory states that Economic growth results from the increasing returns associated with new knowledge or technology. New growth theory makes shift from resources-based to a knowledge-based economy. It underscores the point that economic processes which create and diffuse new knowledge are critical to shaping the growth of business firms. The essential point of new growth theory is that knowledge drives growth. The major assumptions of new growth theory are:-

a. It views technological progress as a product of economic activity whereas previous theories treated technology as a product of non-market forces.
b. It holds that unlike physical objects, knowledge and technology are characterized by increasing returns, and these increasing returns drive the process of growth.

Based on New growth theory, technological advancements like e-business, anti cybercrime systems will definitely boost performance of business firms.

METHODOLOGY

The study took an ex-post facto survey design approach. Ex- post facto design was used because of the Time serial nature of the research. This study was carried out in Konga.Com Abakaliki service point in Ebonyi State Nigeria. The data for this study was secondary data from Konga.com Abakaliki service point. Pearson product moment Correlation coefficient analysis and t statistics were used to test the hypotheses raised.

Table 5 malicious agents victims count report in 2015

Month	Under 20	20-29	30-39	40-49	50-59	Over 60	Total
January	7	12	32	38	50	30	169
February	9	13	35	42	56	31	186
March	13	15	38	48	61	33	208
April	12	17	43	50	65	35	222
May	15	21	46	53	67	37	239
June	17	24	49	58	73	37	258
July	20	29	52	63	79	39	282
August	22	32	57	65	85	40	301
September	25	37	59	70	88	42	321
October	26	39	65	72	93	44	339
November	28	43	69	78	99	45	362
December	32	46	73	82	106	47	386

Source: Konga. Com Abakaliki service point 2016

Table 5 above shows reported cases of malicious agent at Konga. Com Abakaliki service point for the year 2015. Total reported case for the period is with increments over the months. With January 169, February 186, March 208, April 222, May 239, June 258, July 282, August 301, September 321, October 339, November 362 and December 386.

Table 7; victims losses in Thousands of Naira (₦000) in 2015.

Month	Under 20 (₦,000)	20-29 (₦,000)	30-39 (₦ ,000)	40-49 (₦ ,000)	50-59 (₦ ,000)	Over 60 (₦ ,000)	Total (₦ ,000)
January	15	30	35	33	42	39	194
February	19	31	37	38	48	36	209
March	20	29	38	41	55	38	221
April	23	32	39	40	61	40	235
May	25	35	45	43	63	41	252
June	26	37	48	46	68	45	270
July	28	39	52	49	72	48	288
August	32	40	56	55	77	49	309
September	38	41	59	57	84	52	331
October	41	40	64	61	88	55	349
November	46	43	69	65	92	57	372
December	49	48	72	69	95	58	391

Source: Konga. Com Abakaliki service point 2016

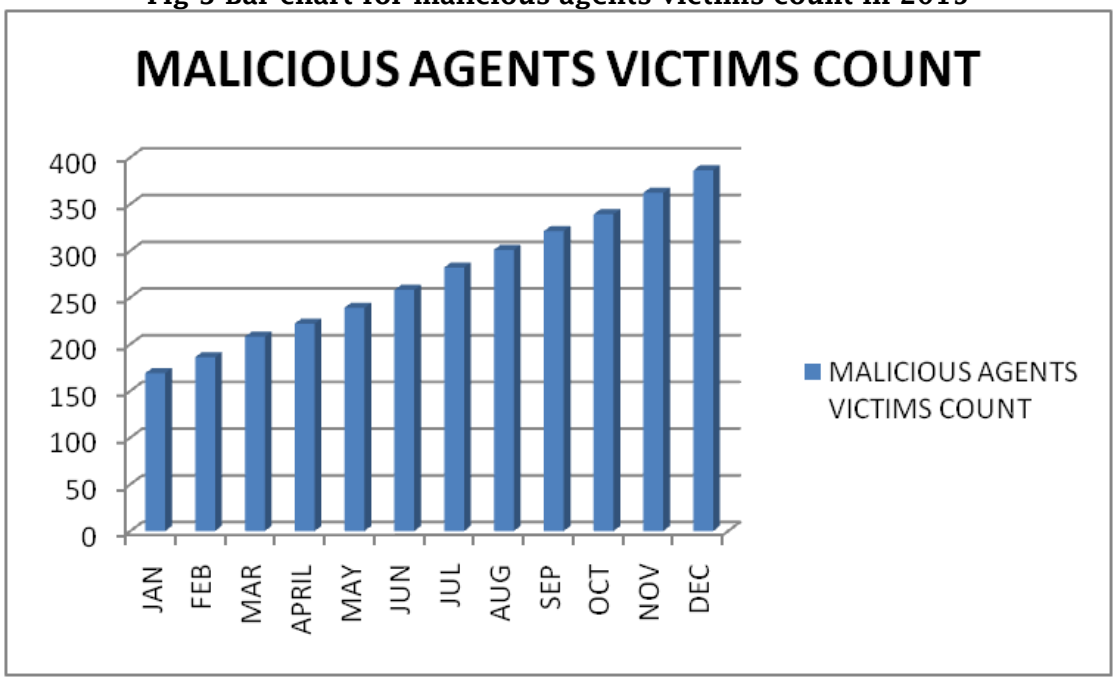
Table 7 above shows the losses suffered by victims of cyber crime in thousands of naira. The monthly losses are: January 194, February 209, March 221, April 235, May 252, June 270, July 288, August 309, September 331, October 349, November 372 and December 391.

Table 9; summary of table 5 reporting malicious agents victims count in 2015

Month	Victims count
January	169
February	186
March	208
April	222
May	239
June	258
July	282
August	301
September	321
October	339
November	362
December	386

Source: Konga. Com Abakaliki service point 2016

Fig 3 Bar chart for malicious agents victims count in 2015



Test of hypothesis 2

Step 1 statement of the hypothesis

Ho There is no significant relationship between malicious agents and performance of E-business websites.

HA There is a significant relationship between malicious agents and performance of E-business website

Step 2 A pearson product moment correlation coefficient analysis was conducted to evaluate the null hypothesis that; there is no significant relationship between malicious agents and performance of e-business websites (N = 12).

Preliminary analysis showed that there was no violation in the assumptions of normality, linearity, and homoscedasticity. There was significant evidence to reject the null hypothesis and conclude that there was a strong positive relationship between

malicious agents (M= 272.75, SD = 70. 59) and losses (poor performance) (M =285.08 , SD = 65.76) r (12) = 0.999, P < .01. Higher levels of malicious agents are associated with higher losses.

Table 14 correlation test result for hypothesis 2

Correlations

		MALAGENTSVICTIMSCOUNT	VICTIMLOSSESNAIRATHOUSANDS
MALAGENTSVICTIMSCOUNT	Pearson Correlation	1	.999**
	Sig. (2-tailed)		.000
	N	12	12
VICTIMLOSSESNAIRATHOUSANDS	Pearson Correlation	.999**	1
	Sig. (2-tailed)	.000	
	N	12	12

**. Correlation is significant at the 0.01 level (2-tailed).

Source; statistical package for social sciences (SPSS 20)

Also a t-test using SPSS 20 gave a calculated t value of 13.337.

Table 15 T-test result for hypothesis 2

Source; statistical package for social sciences (SPSS 20)

	Test Value = 0.999					
	T	Df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
MALAGENTSVICTIMSCOUNT	13.337	11	.000	271.75100	226.9028	316.5992
VICTIMLOSSESNAIRATHOUSANDS	14.965	11	.000	284.08433	242.3021	325.8666

Step 3 H_O is rejected since - $1 \leq r \leq 1$, r = 0.999, andat 0.05 level of significance, the calculated t value 13.337 is greater than the positive critical t value of 1.96. H_A is accepted.

Step 4. There is a significant relationship between malicious agents and performance of E-business website.

Step 5 malicious agents can maximize losses and minimize profit.

This also means that as malicious agent are increasingly introduced in E-business, poor performance(losses) is increasing accordingly. And as malicious agents are inhibited or decreased, poor performance (losses) is decreased. This provides proof to conclude that malicious agents are one of the strong inhibitors for e-business performance and are serious threats to the growth of E-business activities.

The study by [4] conducted on the impact of cyber crime: issues and challenges, further supports the interpretation of hypothesis 2. [8] found a positive correlation between the growth in incidences of crime and the population of a country, and a correlation of crime with the socio-economical and political factors, but most importantly that cyber crime can result to less revenue in the long-term if customers decide not to do business with a company vulnerable to attack.

RECOMMENDATIONS

Given that E-business activities are rapidly increasing in Africa in general and Nigeria in particular, it is very pertinent that adequate security measures are put in place to ensure, confidentiality, integrity of sensitive and important data. Based on these, the following recommendations are suggested:

a. Robust data security through encryption is necessary to ensure the authenticity of sensitive information in E-business activities. This could be achieved through prudent investment in Antivirus technology, efficient backup systems and effective encryption.
b. Innocent E-business users should cultivate the habit of continuous update on their knowledge about the ever evolving nature of ICTs, this will make them more informed about the current trends in cyber crimes. Also, E-business users should not provide personal or financial information to others unless there is a legitimate reason to do so.
c. E-business platforms should also consider the latest Biometric technology to data and information security against the regular password and code encryption amongst other.

REFERENCES

1. Anah, B.H., Funmi, D.L. &Makinde, J. (2012). Cyber crime in Nigerian: causes, Effects and the way out. ARPN Journal of science and Technology. 2(7): 626-631
2. Barnes, D.& Mathew, H. (2007) Searching for e-business performance measurement systems. Electronic journal of information systems evaluation 10(1): 1 – 8.
3. Hansen,G.S. &Wernefelt, B. (2007) Determinants of firm performance: The Relative Importance of Economic and Organizational factors. Strategic Management Journal 1.10(5): 399-411.
4. Kareem, T.S., Owomoyela, S.K. &Oyebamiji, F.F. (2014). Electronic Commerce and Business performance: An Empirical Investigation of Business organizations in Nigeria. International Journal of Academic Research 4(8): 2222 – 6990.
5. Katz, D. & Kahn, R.L .(1966), The social psychology of organizations, (2nd Edition), New York : John wiley and sons publishiers.
6. Konings, J. &Roodhooft, F. (2000) The Effect of E-business on corporate performance: Firm level Evidence for Belgium. Center for Economic studies Belgium. 00(25): 1- 15.
7. Kumar, R. V. (2010). Sampling and sample survey. Xavier institute of social service; India, Ranchi 2010.
8. Olusola, M., Ogunlere, S., Ayinde, S. &Adekunle, Y. (2013). Impact of cyber crimes on Nigerian Economy. The International Journal of Engineering and Science. 2(4): 45-51
9. Pariyani, R. (2013). Online crimes and their impacts: A review. Manupatra journal. 2(1): 3 – 19.
10. Saini, H., Rao, Y.S .& Panda, T.C. (2012). Cyber crimes and their impacts: A Review. International Journal of Engineering Research. 2(2): 202-209
11. Salifu, A. (2008). The impact of Internet Crime on Development. Journal of Financial Crime. 15(4):10-25
12. Sharma, H., Lavania, D. & Gupta, N. (2011). ERP + E-Business = An emerging relationship. International Journal of managing value and supply chains. 2(2):1-9
13. Sumanjit, D. &Nayak, T. (2013). Impact of cyber crime: Issues and challenges . International Journal of Engineering sciences & Emerging Technologies 6(2): 142-153.
14. www.federalbureauofinvestigation.com / internet crime complaint centre. (accessed on 12/12/2016)