12

Relationship between Cybercrime and Good Governance in Tertiary Institutions in Rivers State

DR. FELICIA KING-AGBOTO
Department of Physical Science Education,
Imo State University, Owerri

DR. DANIEL ORIFAMAH
Department of Physical Science Education,
Imo State University, Owerri

And

DR. CHIZOMA CATHERINE OKPARA
Department of Life Science,
Imo State University, Owerri

Abstract

Cybercrime is a crime committed with computer-related with the support of a network to actualize their aims. Students in tertiary institutions have been lured into committing cybercrime due to financial pressure to get quick money and they cut corners. The researchers investigated the relationship between cybercrime and good governance in tertiary institutions in Rivers State. The study adopted a correctional design because it seeks to establish what relationship exists between two or more variables. The population consisted of 1632 final year students in the faculty of education at the University of Port Harcourt. The sample was made up of 264 respondents. An instrument used to collect data was a researcher-made questionnaire titled cybercrime and good governance rating scale (CCGG) was on a four-point Likert type scale ranging from strongly agree, agree, disagree, and strongly disagree. All the 20 -items were either positively or negatively keyed items using I, 2, 3, 4 or 4,3,2,1 réspetvely. The instruments were validated by the researchers. The internal consistency reliability was established using the Cronbach Alpha method and coefficient values of 0.68 and 0.64 were obtained for the two instruments. The research questions were answered using mean and standard deviation while Pearson product-moment correlation was employed to test the research hypotheses to determine whether any relationship exists. The result showed that the challenges of cybercrime in tertiary institutions can be averted by meaningful good governance. It was recommended that training and retraining program should be organized for all the students from time to time to sharpen their skills and acquaint them with modern skills.

Keywords: Cyber Crime, Good Governance, phishing, Internet fraud, Denial of Service attacks, and tertiary institutions.

Today's world is moving towards digitization, the occurrences of cybercrimes on systems can be highly damaging. As technology progresses and more people depend on internet-able services for everyday activities including storing their credit card details and transacting money online, cybercrimes are becoming more than ever. The consequences of these digital attacks are destructive and can cause some serious scathe. Damages made by cyber-attacks are so tremendous especially in schools, as schools are adopting more ways to promote online education through virtual classes and other learning options, the chances of cybercrimes have also increased (Gemraj, 2021). Crime is an aspect of life that all citizens must deal with as it seems to have been around as long as civilization itself. Crime has infiltrated communities for centuries and one assertion is that crime is more predominant in poor inner-city neighbors than it is in equivalents that are more affluent. The issue of crime has been in existence since time immemorial right from the period when Adam disobeyed God in the Garden of Eden to the modern highly complex crime network; the human society has never been devoid of criminal activities. According to Igba, Nwambam, Nnamani, Egbe, & Ogodo (2018).

Cybercrime is a crime that is perpetrated toward individuals or groups of individuals with a criminal motive to deliberately harm the reputation of the victim or cause substantial or mental harm to the victim directly or obliquely. Kaspersky, 2021 stated that Cybercrime is a criminal activity that either targets or uses a computer, a computer network, or a networked device. There is major cause of crime such as lack of education, generational poverty, and being nurtured in a single-parent home that seems to play a spectacular function in criminal activity. According to Igba et al (2018) stated that scholars have attributed that the causes of cybercrime include unemployment, negative role model, lack of adequate policing facilities, and social gratification. The technological advancement in cyberspace has made computers an integral component in national development. Criminal activities within cyberspace are now on a global scale. Olaide & Adewole in Odo & Odo (2015) noted that most of the criminal activities in Nigeria are carried out by the youth. Therefore, it has become imperative to examine cybercrime and good governance. In addition, if the youths are given the required training, the knowledge received will be channeled towards the development of the country. Tertiary education in Nigeria comprises undergraduate, post-graduate, and vocational training. Usually, an individual needs to be admitted into a college, polytechnic, or university to receive tertiary education. It is the most specialized form of education where an individual takes a particular course of study. On completion of the course, the individual receives an academic degree, diploma, or certificate that will help such an individual to be a better human being. The apparent gap between what is acquired in school and the reality of the workspace has been largely attributed to poor learning conditions. No wonder, education in Nigeria is for a person who cannot afford functional education overseas. The breakdown in the quality of education has led youths to unusual behaviors and the reason why students engage themselves in Cybercrime. In Rivers State, there are different types of higher institutions (College of education, polytechnics, and universities both state and federal). These institutions have different systems of administration and policies.

Good Governance is the remedy for the insecurity challenge in Nigeria. It is a system of government based on good leadership, respect for the rule of law and due process, accountability of the political leadership to the electorate as well as

transparency in dealing with government (Odock in Bello, 2019). It is governance that provokes and defines the nature of security. When there is governance failure, the security framework deteriorates. The war against crime can only be won by raising governance standards, that is, cultivating the culture of good governance where the government is responsible and accountable to the people. According to Bello (2019), Cybercrime engagement cannot be separated from good governance. Even so, good governance is a part of effective, visionary, transparent, trustworthy, and credible political leadership whose driving force is an improvement in the collective wellbeing of the citizens through well-conceived effectively implemented economic policies and human development programs.

In the same view, Debarati and Jaishankar in Odo & Odo (2015) stated that cybercrime is a law-breaking charge against individuals or groups of individuals with a criminal motive to deliberately 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 (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS). Computer-related harassment as defined in the U.S computer statutes is a situation where an individual uses a computer or computer network to communicate indecent language or make any suggestion or proposal of that nature or threaten any illegal or immoral act.

Good governance is a system of government based on good leadership, respect for the rule of law and due process, the accountability of the political leadership to the electorate as well as transparency in the operations of government (Odock in Bello,2019) . It is important to know if there is any difference between cybercrime and good governance since each institution possesses a unique or peculiar cooperate culture. There is a linear relationship between cybercrime and good governance in that cybercrime is a dislike for good governance that eventually leads to truancy. Good governance has been in existence for over 50 years in Nigeria. The worst has been from 1999 when the country changed from a military dictatorship to a democratic rule. However, there is that belief that good governance thrives in a democratic government (Kola, 2017). The primordial cause of the lack of good governance in Nigeria is the absence of a visionary leader to lead the country. Most of the leaders Nigeria ever had since the return of democracy in 1990 have been in power to pursue personal, ethnic, and religious ambitions. These leaders had no vision for the good of the nation. (Kola, 2017).

In other words, Cybercrime refers to any form of crime committed by any individual through the use of a computer and network (Matthew in Odo & Odo, 2015). The researchers deemed cybercrime as a process where a person or group of persons defraud another person, group of persons, a community, or even a nation mostly for financial benefit through the use of modern technology. Finally; cybercrime can be averted by good governance.

Types of Cybercrime

Phishing scams:

Markus and Steven in Odo & Odo (2015) that Phishing is a form of social engineering in which an attacker, also known as a Phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic

communications from a trustworthy or public organization in an automated fashion. Usually, these cybercrimes are attached to impersonating trusted and popular brands creating fake social media profiles and rogue websites that lure users into them. According to Brien (2021), Phishing is a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document. These sites copy the visual aspect of the real website to create a sense of security and usually ask to fill forms with personal information to receive some kind of benefit, such as discounts. The most refined of these sites might include malicious scripts that scrape the data out of your browser, without the need for forms. Phishing also means using fake email messages to get personal information from internet users, this information is later monetized, in the worst-case scenario, bank information was stolen. Even if no bank information was given, there are plenty of ways to gain profit from personal information as the Cambridge Analytical scandal proved. From a business perspective, these scams are usually trying to impersonate potential providers. To prevent phishing attacks, it is recommended you pay attention to social media profile names and domains. Do not provide information on websites that are not secure.

Internet fraud:

Guillermo, 2021 stated that internet fraud usually asks people to send money promising a much larger sum in the short term. The most famous one is the "Nigerian" scam, also known as the "419" scam which is the number of Nigerian law breaches. These scams were already distributed through fax, telephone, and traditional mail, but the Internet made them much easier to pull off and more circulated. Usually, the victim receives communication from someone in need of help to move a large sum of money from a foreign country. There are good deals of variations of this scam and more are developed each day. The victim will be asked to cover a small portion of the cost of moving the money or asset and will be promised a bigger cut of the benefits when the process is over. If the victim falls for it and transfers money, he or she will be told that interference has arisen and that more money will be required. Of course, the victim will not recover anything and this will go on until the scammer feels like there's nothing to gain from this victim and jump to another one. Another common fraud is related to fake job listings, where the victim is asked to pay some money to cover the cost of paperwork or pre-on-boarding formation. To prevent internet fraud attacks, it is recommended you make use of common sense because not all that glitters are gold. Distrust unsolicited communications from strangers offering very attractive deals and never pay in advance for any of these (Guillermo,2021).

Denial of Service attacks

According to Marcus (2021), denial of service means sending so much traffic to a computer or network such that its resources are overwhelmed and they are made unavailable to anyone. When affected by a Denial of Service attack, the school would be unable to access and use the affected systems. Denial of Service (DOS) attacks can also happen through the internet. It is carried out by opening many connections to the computer and leaving them open; this consumes plenty of resources on the computer and can crash it. Though internet connection will go bonkers before a crash, it's difficult to detect DOS because its strength lies in bombarding the computer with connection requests at a very high speed. So before you can discover what went wrong, the system

would have already gotten too slow to start monitoring it. To prevent denial of service attacks, a system should be built and configured around the concept of redundancy and the ability to failover to a secondary system if the first is unavailable. (Marcus.2021)

Statement of the Problem

It has been observed that financial pressure has lured people, students, into doing things that ordinary, they should not have done. To get quick money and solve financial pressure, they cut corners. However, when the basic needs are lacking, the agitation would abound. Cybercrime has posed a huge threat to internet users by stealing millions of information from users in recent years. It has also caused a huge dent in the global demand for cyber security is expected to be £170.4 billion by 2022. 95% of cyber security violations occurs due to human mistake according to Cybint in Isha (2021). Cybercriminals have increasingly ravaged tertiary institutions in Rivers State as profitable targets for cyber-attacks. The reasons for infiltrating an institution's network and privacy were to investigate, infiltrate valuable user data such as security numbers, personal identification; information schools keep on students, parents, and staff. Whenever cybercriminals succeed in hacking data, they sell it on the dark web for a profit. This is why schools, health care providers and retailers, and industries are facing cyber-attacks. The youths are leaders of tomorrow and should be given proper education to be able to channel their energy towards more profitable ventures. To curb the menace happening in our tertiary institution, every individual should be engaged for if they are not engaged, they engage in violent activities such as cybercrime, trafficking, and kidnapping. Also, awareness should be created against the pitfalls of cyber threats.

Purpose of the study

Specifically, the purpose of this study were to:

1. Find out whether any relationship exists between Denial of Service and good governance in a tertiary institution?
2. Find out whether any relationship exists between Phishing scams and good governance in a tertiary institution?
3. Determine whether Internet fraud has any relationship with good governance in a tertiary institution?

Research Questions

1. What is the relationship between Denial of Service and good governance in a tertiary institution?
2. What is the relationship between Phishing Scams and good governance in a tertiary institution?
3. What is the relationship between Internet fraud and good governance in a tertiary institution?

Hypothesis

The following null hypotheses were tested at a .05 level of significance and formulated to guide the study.

1. There is no significant relationship between Denial of Service and good governance in a tertiary institution?

2. There is no significant relationship between Phishing scams and good governance in a tertiary institution?
3. There is no significant relationship between Internet frauds and good governance in a tertiary institution?

Methodology

The study adopted a correctional design. The population consists of 1632 final students in the faculty of education at the University of Port Harcourt. The sample was made up of 264 respondents. An instrument used to collect information was a researcher-made questionnaire titled cybercrime and good governance rating scale (CCGG), which was structured on a four-point Likert type scale ranging from strongly agree, agree, disagree, and strongly disagree. All the items that were positively keyed items rated I, 2, 3, 4 and for the negatively keyed items 4,3,2,1. The 20 -items in the instruments were validated by the researchers. The internal consistency reliability was established using the Cronbach Alpha method and coefficient values of 0.68 and 0.64 were obtained for the two instruments. The three research questions were answered using mean and standard deviation while Pearson product-moment correlation was engaged to test the research hypotheses to determine whether exist any relationship.

Results

Table 1: Mean and Standard Deviation Scores of Good Governance and Denial of Service in Tertiary Institutions

Variables	N	Mean	SD
Good governance	**136**	**9.7**	**2.37**
Denial of service	**128**	**9.1**	**3.5**

The table shows that there is a difference between good governance and denial of service. The above analysis shows that students under good governance had a mean score of 9.7 with a population standard deviation of 2.37 while denial of service had a mean score of 9.1 with a population standard deviation of 3.5. Because good governance scored higher than denial of service, however, it is ideal to reduce cybercrime in higher institutions.

Table 2: Mean and Standard Deviation Scores of Good Governance and Denial of Service in Tertiary Institutions

Variables	N	Mean	SD
Good governance	**136**	**9.7**	**2.37**
Phishing scams	**128**	**12.8**	**4.42**

The table shows that there is a difference between good governance and phishing scams. The above analysis shows that students under good governance had a mean score of 9.7 with a population standard deviation of 2.37 while denial of service had a mean score of 128.0 with a population standard deviation of 4.42. Because good governance scored higher than phishing scams, however, it is ideal to reduce cybercrime in higher institutions.

Table 3: Mean and Standard Deviation Scores of Good Governance and Denial of Service in Tertiary Institutions

Variables	N	Mean	SD
Good governance	**136**	**9.7**	**2.37**
Internet Fraud	**128**	**16.0**	**7.43**

The table shows that there is a difference between good governance and internet fraud. The above analysis shows that students under good governance had a mean score of 9.7 with a population standard deviation of 2.37 while internet fraud had a mean score of 9.1 with a population standard deviation of 3.5. Because good governance scored higher than internet fraud, however, it is ideal to reduce cybercrime in higher institutions.

Table 4 Pearson Product-moment Correlation between Good Governance and Denial of Service

Variables	∑	∑2	N	∑XY	R	Df	Standard Error	R critical	Decision
(Y) Good governance	136	1394	264	1268	0.37	12	0.36	2.179	Accept
(X) Denial of service	128	1334							

The table shows that the sum and sum of squares for good governance are 136 and 1394 while that for denial of service are 128 and 1334 respectively. The sum of the product of scores on the two variables is 1268. The computed correlation coefficient is 0.37 which is less than the critical r ratio (2.179) at 12 degrees of freedom and 0.05 level of significance. Therefore the null hypothesis is accepted. There is no statistically significant relationship between good governance and denial of service, r (12) = 0.37, P < 0.5, two-tailed. That is variable Y (good governance) does not vary significantly with variable X (denial of service) among cybercrime. With the correlation coefficient of 0.37, variable X does not account for approximately 0.37 %(ie.57x57x100)of the variance in variable Y. The significance of the r or the acceptance of the null hypothesis depicts that the correlation between the two variables is not statistically less than zero.

Table 5: Pearson Product-moment Correlation between Good Governance and Phishing Scam

Variables	∑	∑2	N	∑XY	R	Df	Standard Error	R critical	Decision
(Y)Good governance	136	1394	264	1295	0.57	12	1.53	2.179	Accept
(X)Phishing scam	128	1814							

The table shows that the sum and sum of squares for good governance are 136 and 1394 while that for phishing scams are 128 and 1814 respectively. The sum of the product of scores on the two variables is 1295. The calculated correlation coefficient is 0.57 which is less than the critical r ratio (2.179) at 12 degrees of freedom and 0.05 level of significance. Therefore the null hypothesis is accepted. There is no statistically significant relationship between good governance and phishing scam, r (14) = 0.57, P < 0.5, two-tailed. That is variable Y (good governance) does not vary significantly with variable X (phishing scam) among cybercrime. With the correlation coefficient of 0.57, variable X does not account for approximately 0.57 %(ie.57x57x100) of the variance in variable Y. The alternate or research hypothesis is that there is no significant relationship between good governance and phishing scam.

Table 6: Pearson Product-moment Correlation between Good Governance and Internet Fraud

Variables	∑	∑2	N	∑XY	R	Df	Standard Error	R critical	Decision
(Y)Good governance	136	1394	264	1295	0.57	12	1.53	2.179	Accept
(X)Phishing scam	128	1814							

Table 3 shows that the sum and sum of squares for good governance are 136 and 1394 while that for internet fraud are 128 and 2434 respectively. The number of cases is 14 and the sum of the product of scores on the two variables is 1262 with a correlation coefficient is 0.15, which is less than the critical value of r(2.179) at 12 degrees of freedom under 0.05 alpha. Therefore the null hypothesis of no significant relationship between good governance and internet fraud is accepted.

Discussion

The result of the study has shown that there is a significant correlation coefficient between good governance and denial of service. Cybercrime (denial of service) engagement cannot be separated from good governance. Many others have also been linked to the governance system. The general view is that peace and security are determined by good governance. However, good governance is a function of effective, visionary, transparent, trustworthy, and credible political leadership whose driving force is an improvement in the collective wellbeing of the citizens through well-conceived effectively implemented economic policies and human development programs. According to Marcus (2021), systems should be built and configured around the concept of redundancy and the ability to failover to a secondary system if the first is unavailable. The system should also be designed with the ability to deal with increased load over the average normal usage. The result of the study indicated that there is no significant correlation coefficient between good governance and phishing. There is a linear relationship between cybercrime and good governance in that cybercrime is a dislike for good governance that eventually leads to truancy. There has been good governance in Nigeria for over 50 years. The worst has been from 1999 when the

country changed from a military dictatorship to a democratic rule. However, there is that belief that good governance thrives in a democratic government Odo (2015). The finding agrees with Markus & Steven (2017) to prevent phishing attacks, it is recommended the email system should have an effective filter, implementing email authentication methods like SPF, DKIM, and DMARC to filter potential spam. Users should also be trained on how to identify potential spam emails before clicking on any links or documents attached.

The study also shows that most of the developmental challenges Nigerians had today are attributed to these leaders who lacked a good vision for the nation (Odo & Odo, 2015).In other words, according to Kaspersky (2021) recommended the following as the best ways to protect your computer and your data. Keep software and operating updated, use anti-virus software and keep it updated, use strong passwords, never open attachments in spam emails, do not click on links in spam emails or untrusted websites, keep an eye on your bank statements, be mindful of which website URLs you visit, contact companies directly about suspicious requests, do not give out personal information

Conclusion

The challenges of cybercrime in tertiary institutions can be averted by meaningful good governance. The significant growth in human history through computer technology has no doubt brought a change in all aspects of life, especially in communication and information technology. Notwithstanding, the embracement of the internet has come with a lot of mixed feelings despite its numerous importance to the undergraduate students at the University of Port Harcourt, and people are valued regarding what they possess and command economically. Conversely, those without economic success are undervalued, and the pressure to achieve success is high despite the harsh financial condition such as poverty amongst others. These necessitated ability of individuals to organize survival strategies and attain economic success by indulging in cybercrime. The perpetrators of cybercrime are not far-fetched; they are our brothers, friends, colleagues, distant relatives, and neighbors who can be broken under appropriate circumstances with the right and positive communication, orientation, education, and empowerment.

Recommendations

1. Government should set up a mechanism to track and investigate the menace of cybercrimes within and outside the institutions.
2. Functional education that is inculcated with vocational skills can be employed to bring back good governance.
3. Personal information should be kept secret and always update from the official vendors.
4. Training and retraining program should be organized for all the students time to time to sharpen their skills and acquaint them with modern skills.from
5. Government should place CCTV security devices around the school.
6. Awareness programs should be created against the pitfalls of cyber threats and fake online activities within the school should be monitored.

References

Bello, Z.A & Ayilara, T.T (2019) the role of science education in Good Governance, peace education & National security in Nigeria. International journal of scientific research in education studies & social development vol. 3, no 1 July 2019

German Technologies limited (2021) Cybercrime in Schools and How can Tech Aid Them? www.gemrajtechs.com

Guillermo (2021) Cybercrime: which ones are the most common threats today?www.redpoints.com/blog

Igba, D.I, Igba, E, C, Nwambam, A.S, Nnamani, S.C, Egbe, E.U &Og do, J.V (2018) Cybercrime among University Underground:Implications on their Academic Achievement. International Journal of Applied Engineering Research ISSN 0973-4562 Volume13, Number 2 pp.1144-1154I.Research. Indian publication

Isha, U (2021) 20 Important types of cybercrimes to know 2021. Jigsaw Academy is a Manipal global education investee company. www.jigsawacademy.com

Kaspersky, A.O (2021)Tips on how to protect yourself against cybercrime www.kaspersky.com/resource

Kola, A.J, Gana, N.N & Olasumbo, I.O (2017) "The lack of good governance in Nigeria and its impact on functional science education" International Journal of Development and Sustainability, Vol.6 No.9, pp.1036-1047

Marcus, O.B.(2021) What are the types of cyber attacks that could impact my school?www.9ine.com/newsblog

Markus, J & Steven, M (2017) Phishing and Countermeasures: Understanding the increasing problem of electronic identity theft. John Wiley & Sons Inc, New Jersey

Odo, L.U (2015), Democracy and good governance in Nigeria: Challenges and prospects", Global Journal of Human –Social Science (F) Vol 15 No.3, pp.1-9.

Odo, C.R & Odo, A. I (2015) the extent of involvement in Cybercrime activities among students in tertiary institutions in the Enugu state of Nigeria. Global Journal of Computer science and technology (Information & Technology) vol 15 issue 3 version 1,0 the year 2015: http://www.researchgate.netpublication.