

# The Impact of Computer Crime on Corporate Profitability in Nigeria (A Study of GT-Bank PLC)

Unachukwu, Chukwuemeka Larry<sup>1</sup> and Agomuo Alozie Callystus<sup>2</sup>

<sup>1</sup>Department of Industrial Relations and Personnel Management College of Management Sciences Micheal Okpara University Agriculture, Umudike

<sup>2</sup>head of Registry, Economic Community of West African States (ECOWAS) Commission, Asokoro, Abuja

---

**Abstract:** *This research work critically examines the impact of computer crime on the profitability of corporate organization in Nigeria, using Guarantee Trust Bank (GTB) Aba – Owerri Road, Aba as the study. Both primary data and secondary data were used, the primary data were sourced using a well structured questionnaire which were ministered to the target audience secondary data were source from textbooks, journals, periodicals etc. two level of data analysis were made; description (analysis was done using simple percentage while the inferential analysis was done using chi-square test. It was found out that a computer crime free organization will maximize profitability of such organization. It was concluded the compute crime should be eliminated or reduce to the barest level in every organization. It was therefore require for companies to adopt a constant and realizable quantities approach toward eliminating computer crime in organizations in Nigeria.*

**Keywords:** *Computer crime, corporate profitability*

---

## INTRODUCTION

Computer crime otherwise known as Electronic or Cyber crime generally refers to the criminal activities done using the computer system or Network. Although computer crime most a time is restricted to describing criminal activities in which the computer or network is a necessary part of the crime, these terms are also sometime used to include traditional crime committed with the aid of the computer such as fraud, theft, blackmail, forgery and embezzlement. Many countries all over the globe face the menace of criminal activities committed using the computer or network, committed using the computer or network, people are tracking into the database of an organization if not strongly secured with a strong pass ward difficult to be backed including corporate organization in Nigeria. Computer crime can be broadly defined as a criminal activity involving an involving an information technology infrastructure which an illegal access (unauthorized access), illegal interception (by technical means to access non-public data transmission form or within the computer system). Data interference, unauthorized access, damaging, detection, deterioration, alteration or suppression of computer data can be a threatening effect and damages of not properly check.

However, computer saves a lot of time been wasted by manual system to verify claims for payment and cash withdrawal in banks. These encourages and at the same time increase customers confidence in the bank and made available useful time in verifying procedure for more banking operations.

Developing countries like Nigeria sequel to the numerous advantages of the computer system, the banking sector and all other sector in the economy adopt the idea of making every transaction computerized; this reduce in work load and time saving necessitates the adoption of the system in most sectors. The level of corruption in the society makes the numerous advantage of the system to have a big loophole because of crimes committed using the computer system.

Additionally, GT-Bank plc has been one of the new generation but highly reliable banks in Nigeria because of their guaranteed service to their customers. They will among others find this research work of great help, in that it focuses on the impact of computer crime in the profitability of corporate organization. If the measures pointed out will be strictly applied, it will go a long way in checking and minimizing criminal activities and the rates of computer crime will be reduced in banks.

## **BACKGROUND OF THE STUDY**

Introduction of computer in the banking industries has helped in revolutionizing the banking sector. Cyber crime is one of the words frequently used by individuals in our contemporary society. The term “cyber” is a prefix used to describe an idea as a part of the computer and information age. Crime can be described as any activity that contravenes legal procedures, mostly performed by individuals with a criminal motive. Cyber crime also known as computer crime is seen as offence that are committed against individuals or groups of individual with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly through a modern telecommunication network such as internet and mobile phones. Such crime may threaten a nation’s security and financial health.

The internet has offered a lot of platform for useful research purposes; however, computer crime is a world-wide problem that is costing companies billions of naira. According to crime research.org, as early as 2003, guarantee trust bank was leading the banking sector in the percentage of cyber attack at 35.4%. Banks with high rate of cyber crime started as a result of many hackers and other cyber criminals flourishing in countries with few internet crime laws while attacking richer countries through their computer because, it lacks rules and codes of a central authority which governs it as such internet has no global demarcation (as remarked by guidance and fortieth 2003). In Nigeria, cyber crimes are performed by people of all ages, ranging from young to old, but in most cases, the young. Several youth engages in cyber crime with the aim of emerging as the best hackers or as a profit making venture since the tools for hacking in our modern world has become affordable by many.

Records scan it made possible as a result of the large number of young people who now see cyber crime as a source of livelihood. This study tends to look at cyber crime, its impact, and effects and suggest ways to combat such crimes as it affects guarantee trust bank and other establishment as well.

### **OBJECTIVE OF THE STUDY**

This research work generally aims at evaluating the impact of computer crime on the profitability of corporate organization in Nigeria. Specifically, the study aims to achieve the following:

- Evaluating the effectiveness of computer security in Banks.
- Determine the possible ways of tracking hackers and also preventing hackers from the system.
- Evaluate the impact of profit dilution in the organization.
- Determine whether the system database is strongly secured, also the possible strong data password determination.
- Ensuring and evaluating the internal control of the organization.
- Evaluating the viability of antivirus used by the organization.

These and many more are problems identified to be tackled in the process of this research work and possible solutions given.

### **REVIEW OF RELATED LITERATURE**

As digital technology advanced over the past 50 years with a huge unprecedented advancement in history, government, business and people around the globe have been affected immeasurably. The already enormous and exponentially, fraud capacities for electronic storage, transmission and rapid manipulation of binary data changed the landscape virtually overnight (according to Balettrack 2009). Galaner (2000); he described computer as a device that accept information of one kind or another, stores it according to a carefully prepared set of rules or procedures, and then dump it out in a new form. But the fear that computer will violate the right to piracy and results in a society were human being no longer think capacity for themselves is certain.

According to Charles (2013); computer is seen as an electronic device that accepts data as an input, process the data to give accurate output called information. Dimoji (2014); defined computer crime as unethical behavior exhibited by people using the facilities provided by information technology environment to defraud the company. Computer crime also known as cyber crime according to Nwosu (2012) refers to the criminal activity where computers or network is the source, target or place where the crime is committed. These categories are not exclusive; any activity can be classified as computer crime if it is done using any information technology facility to cause harm. There are also hacking activities directed towards individuals, families and industries such as banks, organized by group within the network rendering services or signal. According to Jones (2000) on 3<sup>rd</sup> August 2000, federal prosecutors charge mafian boys with 54 count charge for illegally assessing the computing computer plus a total of 10 counts of mischief of data for his attack on Amazon. Dell computer outlaw and yahoo

mafian boys have also attacked other website, but, prosecutors decided that a total of 66 counts were enough.

About 50 computer at Stanford University and also computers at the University of California at Barbara were amongst the zombie computer sending pins in DOS attack. In early March, 2011, a company named Honeywell was hacked by computer fraudsters and important document relating to the company was copied and sent to another company who needed such information to compete with the company favorably.

### **TYPES OF COMPUTER CRIME**

According to Dimoji (2014); there are primarily many types of computer crimes in practice by fraudsters, multiple crimes that are concurrent, or, lesser offences that can occur during any given criminal transaction resulting in an overlap between the classification which includes the following:

- Cyber crime
- Malware and Malicious code
- Denial of service attacks
- Computing virus
- Information warfare
- Cyber stalking
- Fraud and identity theft
- Fishing
- Virtual crime

According to Newsweek, government officials and security specialists have documented a significant increase in internet probes and server scans since early 2001 because of the crimes committed using the computer system. According to Oduveme (1998), banking regulation in Nigeria and analytical perspective describes cyber terrorist as someone who intermediates companies, governments to advance his/her political or social objective by launching computer based attack against computer network and the information stored in them.

### **MANIFESTATION FORMS AND WAYS OF COMMITTING CYBER CRIME**

The following are ways and forms computer crime can be committed according to Dimoji (2014):

- Computer trickery
- Financial theft and misuse
- Forgery of data and document
- Making and use of computer virus
- Computer sabotage and espionage
- Hacker ship

### **MAKING USE OF COMPUTER VIRUS:**

Computer virus are software programs, which are made by indispensable individuals to cause damage to many computers connected in networks, for example, the internet, and are considered one of the most powerful weapons of cyber criminals. Basic characteristics of these programs are:

- i. They copy themselves into each computer they come in contact with.
- ii. They are noticeable; i.e. users often do not know about them especially if a program for virus scanning is not installed.
- iii. They automatically do some commands like detecting useful data out of the victim's computer, or sending data to other locations in the network, about which he owner of the computer does not know.

### **METHODOLOGY OF THE STUDY**

#### **PREAMBLE**

This research is made up of different techniques in order to help the researcher to get the necessary result he is looking for.

#### **AREA OF THE STUDY**

This research work is an empirical investigation into the impact of computer crime on corporate profitability. Before a good research work could be obtained, there is need for the researcher to state clearly the terms, methods and procedure adopted in the course of gathering the facts which is critical to the success of any research work. The work is coordinated in GT-bank, Abe-Owerri road.

According to GT-bank annual report, the criminal intent measuring a specific computer crime which may be difficult to prove; how does an investigator distinguish between hackers who intentionally steals or destroys electronic file and someone who accidentally destroys file while simply working on them?

## **PRESENTATION AND ANALYSIS OF DATA**

### **INTRODUCTION**

This chapter reflects the investigation made by the researcher. Findings in the study are based on the response gathered on the questionnaire, relative interview questions and information gathered from other source which is material to the study.

The researcher adopted strategies devoid of undue influence to gather the information from all the workers in guaranteed trust bank (GTB).

Also, this chapter encompasses the data presentation, test of hypothesis, discussion of findings.

### **PRESENTATION OF DATA**

Here, the relevant questionnaire collected will help the researcher to draw conclusion on the topic of his study. The questionnaire collected from respondents is represented with table and chart also using chi-square. 80 questionnaires were administered while 70 submitted on time; below are the representation of the data responded from few questions asked by the researcher.

#### **Classification of respondent based on sex**

**Table 4.1 sex of respondent**

<b>Option</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>Total</b>	<b>Percentage (%)</b>
Males	10	15	5	30	45
Females	10	15	15	40	55
Total	20	30	20	70	100

The table shows that 30 respondents representing 45% were male, while 40 respondents representing 55% were female.

#### **Question 1**

How effective is the company (bank) data base?

**Table 4.2 response to the question**

<b>Option</b>	<b>Junior Staff</b>	<b>Middle</b>	<b>Senior</b>	<b>Total</b>	<b>Percentage (%)</b>
Yes	15	28	7	50	75
No	5	12	3	20	25
Total	20	40	10	70	100

Key: Yes – very strong

No – not to strong

The table above shows that 50 respondent representing 75% says yes while 20 respondents representing 25% of the respondent says no that the database of the computer is not effective.

**TESTING OF HYPOTHESIS**

The following hypothesis formulated earlier will be tested below using the chi-square.

- Ho: There is existence of expert rate management of the data base.
- Ha: There is no existence of expert rate management of the data base.
- Ho: There are strong internal control measures in the company.
- Ha: There are no strong internal control measures in the company.
- Ho: Computer crime does not affect the profitability of corporate organization.
- Ha: Computer crime affects the profitability of corporate organization.

**TESTING HYPOTHESIS 3**

Option	Junior Staff	Middle	Senior	Total
Yes	12 (1)	4 (2)	20 (3)	36
No	18 (4)	0 (5)	16 (6)	34
Total	30	4	36	70

Calculating the expected frequencies using

$$E_{ij} = \frac{R_i \times C_j}{N}$$

$11 = \frac{36 \times 30}{70} = 15.43$   
 $12 = \frac{36 \times 4}{70} = 2.06$   
 $13 = \frac{36 \times 36}{70} = 18.50$   
 $21 = \frac{34 \times 30}{70} = 14.57$   
 $22 = \frac{34 \times 4}{70} = 1.94$   
 $23 = \frac{34 \times 36}{70} = 17.49$

Calculating for chi-square

$$\chi^2 = \sum \frac{(O_y - E_y)^2}{E_y}$$

$O_y$  = observed frequencies  
 $E_y$  = expected frequencies

Oy	EY	Oy - EY	(Oy - EY) <sup>2</sup>	$\frac{(Oy - EY)^2}{EY}$
12	15.43	-3.43	11.76	0.76
4	2.06	1.94	3.76	1.83
20	18.50	1.50	2.25	0.12
18	14.57	3.43	11.76	0.81
0	1.94	-1.94	3.76	1.94

6	17.49	-11.49	132.02	7.55
				13.01

Calculating the test statistic of critical value at 5% level of significance

Degree of freedom:-

$$(R - 1) (c - 1)$$

$$(2 - 1) (3 - 1)$$

$$1 \times 2 = 2$$

Therefore, critical value at 5% level of significance =  $0.05 \chi^2 = 5.99$

### **Interpretation of result**

From the tested hypothesis using the decision rule formulated since  $\chi^2$  calculated equals 13.01 and critical value equals 5.99 we accept the alternative hypothesis and conclude that computer crime affects the profitability of corporate organizations.

## **SUMMARY, CONCLUSION AND RECOMMENDATION**

### **CONCLUSION**

From the discussion of finding and having gathered information necessary for this study, the research conclude that steps must be taken by the organization to minimize or eliminate computer crime because it affects the profitability of any organization. In case, any information is stolen from the system, there should be adequate attention to how the information disappears in the system because, if hacked, there must be a trace.

On the other hand, from the information and judgment gathered so far in the course of this study, computer crime has played a very big role in determining the profitability of corporate organization. Following the trend of things in an organization, it was observed that recommendations are made which when implemented would assist the company in detecting and preventing computer crime in the company. It was observed that many organizations or industries have ceased to exist because they have ignored the impact of computer crime on the profitability of firm thereby jeopardizing and narrowing their chances of success in the competitive industry.

### **RECOMMENDATION**

Having itemized the discussion of findings of computer crime on profitability, the impact of which it has been well felt, we have come to establish the fact that positive impacts outweighs the negative impact on that note, therefore, more effective utilization of the positive effect on the profitability "computer crime free environment" is considered achieving the set goals of the company based on the findings, we recommend the following:

That the company should engage adequate qualified personnel to manage the company's database and also trace incidence of hackers in the system so that perpetrators can be brought to book. Failure to do this management instruction can spell doom for any organization concerned irrespective of size or finance strength.



Strong password should be developed and used to secure the database of the company not just forming a password that can be broken by hackers. Failure to do this will expose the company's information to the third party which can be the rival company. Having seen the importance of strong internal control in any organization, the management should develop a strong internal control measure in the organization to check fraud mostly, teeming and lading in the organization, as well as combine computer crime. These will help reduce the rate of criminal activities in the organization. Also, there should be back up to all the company's relevant information to avoid loss of data upon any eventualities. This will enhance corporate productivity as information loss in the system can be retrieved from the backup. Finally, the management of the company should formulate policies to guide and checkmate computer crime in the organization.

### **SUGGESTION FOR FURTHER STUDY**

This study was limited to only Aba – Owerri road branch of the bank GTB. In the light of this research should be carried out on a wider scale and on other branches and other banks in Nigeria. The research would want to suggest that further research work should be carry out on the impact of management decision in he computer crime in a corporate organization. The researcher would want to suggest that further research, work should be carry out on the impact management decision on the computer crime in the corporate organization in Nigeria. Also, study should also be conducted on the adequacy of computer programs maintenance in a corporate organization. Finally, come area's of the computer system and networking including prevailing accounting packages should be studied to enhance the efficiency and effectiveness of the study to corporate organization is Nigeria.

### **BIBLIOGRAPHY**

- Benson E.M and Oju O. (2012); computer package for business management: chimera publication, Aba.
- Dimoji O. and Oju O. (2013); comprehensive guide to proessional practice in technology development: Onyi graphic press, Aba.
- Dimoji O. (2010); computer programming for higher learners: Kayee publication, Aba.
- Olowe R.A (1998); financial management and computer activities: Brerly Jones publication, Lagos.
- Ogbulu O.M (2002); lecture notes on computer crime and other related activities: ABSU
- Okpara G.C (1995); cyber crime, debating the meaning and significance of cyber crime in an organization, new media and society Vol. 5(3)
- Paul H (2002); wireless road inks, the complete guide to wireless computing and networking: Chicago alpha books.
- Lagram A and Stewart J (2003); configuring the internet access in a café environment: New media Vol. 7(4)
- Walter G and Waller V (2006); the internet companion: the easy Australian guide Canbarra, UNS press.