# Journal of Internet Banking and Commerce

*An open access Internet journal (http://www.arraydev.com/commerce/jibc/)*

*Journal of Internet Banking and Commerce, April 2010, vol. 15, no.1*
(*http://www.arraydev.com/commerce/jibc/*)


## Computer Crimes and Counter Measures in the Nigerian Banking Sector


**Olasanmi, Omoneye Olufunke, Lecturer**
**Department of Management and Accounting, Faculty of Administration, Obafemi Awolowo University, Ile-Ife, Nigeria**
*E-mail:* **neyeolasanmi@yahoo.com**


Olasanmi Omoneye O. is a lecturer in the Department of Management and Accounting, Faculty of Administration, Obafemi Awolowo University, Ile-Ife, Nigeria. Her areas of interest include E-commerce, Management Information Systems, Electronic Marketing, and Information Systems Security. She is currently carrying out analysis on issues relating to IT innovations and customer satisfaction. Her publications include areas such as e-governance, ICT sustainability, and e-education.


### Abstract

The increase in the use of the information and communication technology (ICT) facilities such as computers and the Internet in the perpetration of criminal activities like spamming, credit card frauds, ATM frauds, phishing, identity theft, denial-of-service, and a host of others has lend credence to the view that ICT is contributing to crime in the banking sector. A greater understanding of such computer crimes may complement existing security practices by possibly highlighting new areas of counter measures. This paper thus assesses whether these crimes can be totally eradicated or not and whether the new generation banks experience more computer crimes than the old generation banks in Nigeria. Based on the findings of this study, the paper concludes that total eradication of computer crimes is not possible but can be highly reduced if internal control measures are adequately put in place within a bank's organizational structure and that new generation banks seem to experience more crimes than their old generation counterparts due to the fact that majority of their services, which are automated, are subjected to technological changes at a rapid rate.

Key Words: **Computer crimes, Control measures, the Internet, ICT**



## INTRODUCTION

As much as the computer has been used to improve the mode of operations in the different sectors of the society, it has also evolved as a medium for some people to commit crimes. It started in the 1960's in the form of hacking as a means of solving problems and then in the 1970s, computer crimes such as privacy violations, phone tapping, trespassing and distribution of illicit materials were experienced. Software piracy, copyright violations, and the introduction of viruses were added to the list in the 1980s. Things went downhill and now, the extent of the damage caused by computer crimes is monumental; the international market has not been left out with computers being used for espionage and transnational organized crime and terrorism. Computer crimes have become a major source of concern for organizations worldwide.

When banks and other organizations began to be computerized in Nigeria over a decade ago, little did they know that they were setting the pace in computer crimes age. Today, the computer is used everywhere, with individuals and corporate bodies having now found its use compelling. With its usage, the computer and the Internet have changed working attitudes in the banking industry. If there is anything that has necessitated the use of computers in banks, it is the large number of transactions they process. Since banks handle large numbers of transactions on a daily basis, the use of computers and the Internet have become inevitable.

Essentially, computers and the Internet in banks facilitate records of customers' transactions and transfer of monetary values. With the computer and Internet facilities put in place, customers communicate directly with their banks to pay bills, transfer funds, inquire about account balances, and perform all sorts of services offered by such banks. This development is extremely profitable to all but organizations employing computers and the Internet to improve business processes should not ignore the fact that it also improves efficiency both for the company and the criminally-minded.

It should be noted that before the development of computer crimes, there had been occurrences of bank-related crimes. These traditional crimes include the typical ones such as bank robbery, false statements to a bank in order to obtain a loan, misapplication or embezzlement of bank funds, false entries in a bank's books, bank bribery and bank fraud. There is a marked difference between these traditional crimes and the modern-day computer crimes, as some of the traditional crimes require violence or a threat of violence. In addition, the perpetrators of traditional crimes were more visible and detection of such crimes was relatively easy. Inasmuch as the characteristics of these crimes are different, the motivations of the criminals are much the same; people still rob banks because they need the money stored there. The advent of the computer has only provided another means and opportunity to such criminals.

## STATEMENT OF THE PROBLEM

The computer was invented to hasten data processing with effortless ease. However, as the understanding of the use of the computer has increased across various levels of knowledge, so as its use for committing crimes increased. Today, not only young whiz kids hack into computers, Information Technology (IT) professionals have joined the league. A new breed of white collar criminals has emerged. More mature offenders, often with a background in the IT industry, are infiltrating systems one way or the other. The introduction of the Internet has heightened the threat of these crimes. Everyone is susceptible to computer crimes once you have a computer and a direct or indirect access to the Internet.

Recent changes in technology arising from the convergence of communications and computing are truly breathtaking, and have already had a significant impact on many aspects of life. Banking, stock exchanges, air traffic control, telephones, electric power, and a wide range of institutions of health, welfare, and education are largely dependent on IT and telecommunications for their operation. According to Edwards (1995), “we are moving rapidly to the point where it is possible to assert that ‘everything depends on software’”. The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its cost, has brought about revolutionary changes in commerce, communications, entertainment, and education. Along with this greater capacity, however, comes greater vulnerability. Information technology has begun to provide criminal opportunities of which the olden days criminals would never have dreamed.

The increasing rate at which systems can connect together to share information has not only increased the number of prospective victims of computer-related crime, it also increased the number of prospective offenders. Yet the complexity of these crimes and the elusive nature of computer criminals have made it increasingly difficult to detect or prevent these crimes. Computer crimes have quickly increased in recent years and have overtaken the ability of the government and the various sectors to fully protect their systems.

Estimating the incidence, prevalence, cost, or some other measure of computer related crime is a difficult challenge because such crimes are not easily detected and even when detected, reports to the appropriate authorities are not always made. Businesses do not always want to report problems because there is a perception that their information will be disclosed publicly, which could, in turn, cause harm to their business. Effective responses are therefore required to tackle the issue of computer crimes, particularly given its global dimensions on the Internet.

## OBJECTIVES OF THE STUDY

This research work seeks to bring to light the dangers or threats, possible counter measures and control of computer crimes in the banking sector. The objectives of this study are to:

i. determine the types of computer crimes experienced by some selected banks
ii. identify the factors contributing to the occurrence of such crimes

iii. identify the most prevalent of the computer crimes
iv. proffer control measures to curb computer crimes

## HYPOTHESES OF THE STUDY

***$H_o$:*** *Old generation banks do not experience more computer crimes as new generation banks*

***$H_o$:*** *Computer crimes cannot be totally eradicated in banks*

## DEFINITIONS

A computer crime is an illegal activity that is executed via a computer. It is an act committed in violation of criminal or civil codes using electronic or digital technologies for unauthorized activities and transactions. It involves access to the whole or any part of an Information Technology system without right. In the banking sector, it could mean manipulating banking systems to make unauthorized identity theft with reference to ATMs.

Computer crime is a crime in which the use of or access to a computer or its components (terminals, networks and so on) is an essential element; that is, the crime could not have been committed without the use of a computer. Computer crime mainly consists of unauthorized access to computer systems, data alteration, data destruction, or theft of intellectual property. Almost all computer crimes involve unauthorized access or access exceeding the authorisation. The hacker, by stealing or bypassing the password and other security features, breaks into the computer system. The intention may be to commit financial fraud or to steal some sensitive data.

Computer crimes are usually targeted at networks (generally defined as a specific type of relation linking a defined set of persons, objects, or events). Technology creates dependencies that evolve to interdependency; a significant attack on one can directly impact others (cascade effect). Computer crimes have quickly increased in recent years and have overtaken the ability of the government and the private sector to fully protect their systems. The introduction of the internet has heightened the threat of these crimes. Not only does the increasing connectivity increase the number of prospective victims of computer-related crime, it also provides prospective offenders with greater access and wider opportunities.

## CHARACTERISTICS OF COMPUTER CRIMES

A computer crime is very similar to a normal crime. The only difference is the means in which the act is carried out. An individual can commit theft, trespassing, embezzlement and fraud all on a computer system.

a) Invisibility/Anonymity of offender**:**
   Tracing perpetrators of these crimes require a degree of computer know-how that is usually lacking in most organizations. These criminals are not like the traditional criminals that physically rob a bank; pin-pointing who exactly is committing such crimes is extremely difficult.

b) Lack of victim awareness:
In most cases, victims of theses crimes are not even aware that they have been infiltrated. An individual with a personal computer might not even know when his/her system has been infected with a virus or when his/her account has been tapped into. It is much worse for large organizations because they don't usually have adequate monitoring systems that can detect such crimes.

c) Unwillingness to report:
Most organizations tend to put a lid on the crimes being perpetrated in their organization for various reasons such as to avoid negative publicity, incidents not serious enough, or their company was not specifically targeted etc.

d) Intangibility of digital goods, evidence, value:
Computer crimes can be seen as virtual crimes; they can't be touched. The criminal is not seen physically committing the crime, the goods being stolen are not physical good and prosecution for these crimes is difficult as there is no tangible evidence to present.

## CONTROL AND PREVENTION OF COMPUTER CRIMES IN BANKS

Banks have to decide what security measures they are prepared to invest in and what trade-offs they are prepared to make when it comes to computer crimes. Computer crimes are fast and growing because the evolution of technology is fast, but the evolution of law is slow. Controls can be instituted within industries to prevent such crimes. Protection measures such as hardware identification, access controls software and disconnecting critical bank applications should be devised. However, it should be noted that computers don't commit crimes; people do. The perpetrator's best advantage is ignorance on the part of those protecting the system. Proper internal controls reduce the opportunity for fraud.

While a variety of countries are passing legislation relating to computer crime, the awareness of the situation is still lost on our own government. To be able to effectively tackle this problem, organizations need to make the public aware of their crime experiences.

## RESEARCH METHODOLOGY

Most computer-related crimes are prevalent in cities with predominantly literate individuals since some level of literacy and intelligence are required to commit such crimes. Thus, the study area will thus focus on a town with big institutions and major banks. Eight banks are purposively selected for this survey, four banks representing new generation banks while the other four represents old generation banks. Data for the study is collected through the administration of questionnaires and unstructured interviews with some workers of the selected bank.

**Data Analysis Technique**

Data collected was analyzed using SPSS software, version 15. The analysis method included frequency tables, pie charts, bar charts, and cross-tabulations while Chi-square was employed as the inferential analytical tool for the testing the hypotheses of the study.

Data was gathered from 40 respondents using the purposive sampling method. Purposive sampling method is a form of non-probability sampling in which the population elements are intentionally selected purely at the discretion of the researcher. The power of purposive sampling lies in selecting information rich-respondents for in-depth analysis related to the central issues being studied (Trochim, 2006). These respondents have one time or the other experienced computer crimes, perpetrated within or outside the bank premises by either customers or bank workers.

Of the 40 respondents selected for the study, 30 respondents (75 percent) actually participated in the research. The remaining 25 percent (10 respondents) were either unwilling to take part in the research or were too busy to fill the questionnaire; the unwilling ones opined that their responses might view their banks in a bad light and opted out of the research.

83 percent of the respondents acclaimed that they have experienced some forms of computer crimes. 22 percent of the respondents indicated that the crimes experienced were perpetrated by people outside their organization while 33 percent indicated that the crimes were perpetrated by internal members. 36 percent believed that the internal crimes were carried out to illicit financial gains and to settle some personal grievances within the banking arena. 53 percent of these crimes were often carried out through the Automated Teller Machine (ATM), 34 percent through Internet access, while 13 percent were executed on computer systems files.

The highest form of these crimes is internet fraud (15 percent), followed by information forgery and counterfeiting (13 percent) and computer facilitated financial fraud (12 percent). Other crimes include hacking by outsider (9 percent), virus/Trojan infection (5 percent) and denial of service (3 percent). These crimes caused the organizations huge financial losses and even loss of customers.

**FINDINGS**

| **Variables** | Responses | |
|---|---|---|
| | N | Percentage |
| *Factors contributing to computer crimes* | | |
| Lack of network control | 3 | 11.1% |
| Poor security culture in organization | 3 | 11.1% |
| Lack of security technologies | 2 | 7.4% |
| Inadequate HR for system handling | 2 | 7.4% |
| Inadequate staff training & education in security practices & procedures | 2 | 7.4% |
| Exploitation of insider knowledge or access | 5 | 18.5% |

| | | |
|---|---|---|
| *Security technologies available in banks* | | |
| Physical security | 6 | 15.0% |
| Anti-virus software | 12 | 30.0% |
| Digital IDs or certificates | 2 | 5.0% |
| Encrypted files | 3 | 7.5% |
| Intrusion detection systems | 3 | 7.5% |
| Firewalls | 4 | 10.0% |
| Access control | 10 | 25.0% |
| *Computer crimes detected in banks* | | |
| Abuse of Internet access (Internet fraud) | 9 | 15.2% |
| Unauthorized access to information by insider | 4 | 6.8% |
| System penetration by outsider | 4 | 6.8% |
| Theft of laptop, computer hardware or devices | 4 | 6.8% |
| Virus, worm or Trojan infection | 3 | 5.1% |
| Web site defacement | 2 | 3.4% |
| Computer facilitated financial fraud | 7 | 11.9% |
| Theft or breach of confidential information | 2 | 3.4% |
| Hacking | 5 | 8.5% |
| Information forgery and counterfeiting | 8 | 13.6% |
| Denial of service | 2 | 3.4% |
| Electronic Money Laundering | 4 | 6.8% |
| All of the above | 5 | 8.5% |
| *Measures to control computer crimes* | | |
| Management support in addressing security issues | 7 | 17.5% |
| Adequate training of security personnel | 6 | 15.0% |
| Adequate training of IT personnel | 8 | 20.0% |
| Accurately prioritizing information security against other business needs | 3 | 7.5% |
| Keeping up to date with changes in technology | 10 | 25% |
| All of the above | 6 | 15.0% |

**Hypothesis Testing**

***Hypothesis 1 ( $H_o$): Old generation banks do not experience more computer crimes as new generation banks***

**Cross-tabulation between type of bank and experience of computer crime**

| | | Bank experienced computer crime | | Total |
|---|---|---|---|---|
| | | Yes | No | Yes |
| Type of bank | New | 86.7% | 13.3% | 100.0% |
| | Old | 80.0% | 20.0% | 100.0% |
| Total | | 83.3% | 16.7% | 100.0% |

Level of significance = 0.05
Decision Rule: Reject the null hypothesis if $\chi^2 \geq 6.635$ where

$$\aleph^2 = \frac{\Sigma(O_i - E_i)^2}{E_i}$$

and 6.635 is the value of $\chi^2_{.05, 1}$

| $O_i$ | $E_i$ | $O_i - E_i$ | $(O_i - E_i)^2$ | $(O_i - E_i)^2 / E_i$ |
|---|---|---|---|---|
| 12 | 11.67 | 0.33 | 0.1089 | 0.009 |
| 2 | 2.33 | - 0.33 | 0.1089 | 0.047 |
| 13 | 13.33 | - 0.33 | 0.1089 | 0.008 |
| 3 | 2.67 | 0.33 | 0.1089 | 0.041 |

$\chi^2 = 0.105$
Since $\chi^2 = 0.105$ is less than 6.635 (i.e. $\chi^2 \leq 6.635$), the null hypothesis is accepted, hence we conclude that old generation banks do not experience more computer crimes than new generation banks.

***Hypothesis 2 ( $H_o$): Computer crimes cannot be totally eradicated in banks***
Level of significance = 0.05

**Cross-tabulation between type of bank & possibility of computer crime eradication in banking sector**

| | Possibility of computer crime eradication in banking sector | | |
|---|---|---|---|
| | Yes | No | Total |
| Type of bank New | 7 | 4 | 11 |
| Old | 8 | 5 | 13 |
| Total | 15 | 9 | 24 |

Decision Rule: Reject the null hypothesis if $\chi^2 \geq 6.635$ where

$$\aleph^2 = \frac{\Sigma(O_i - E_i)^2}{E_i}$$

and 6.635 is the value of $\chi^2_{.05, 1}$

| $O_i$ | $E_i$ | $O_i - E_i$ | $(O_i - E_i)^2$ | $(O_i - E_i)^2 / E_i$ |
|---|---|---|---|---|
| 7 | 6.88 | 0.12 | 0.0144 | 0.002 |
| 4 | 4.13 | -0.13 | 0.0169 | 0.004 |
| 8 | 8.13 | -0.13 | 0.0169 | 0.002 |
| 5 | 4.88 | 0.12 | 0.0144 | 0.003 |

$\chi^2 = 0.011$

Since $\chi^2 = 0.011$ is less than 6.635 (i.e. $\chi^2 \leq 6.635$), the null hypothesis is accepted, hence we conclude that computer crimes cannot be totally eradicated in Nigerian banks.

From the data gathered from the respondents in Ile-Ife metropolis, it is evident that most banks have at one time or the other experienced computer crimes in one form or the other. The exact rate of crimes experienced by each bank and the banking sector as a whole cannot be accurately measured at this point, as most banks do not report the computer crimes detected for publicity reasons. These crimes are not being perpetrated by outsiders only, in fact, majority of the perpetrators are reported to have an insider working with them. The perpetrators of these crimes are successful most of the time not just because of their know-how but some organizations make it easy by neglecting staff training and knowledge about computer security or not investing in the right technological equipments. Also, some bank customers aid the occurrence of these crimes by being lackadaisical about their bank accounts, ATM cards and personal information, thereby making themselves easy targets for offenders. Bank customers have to be more careful about the bank's properties in their care.

A major challenge of the banking organization is keeping up to date with changes in technology in spite of the fact that they keep increasing their expenditure on computer security; it seems not to be adequate to cope with the rate of changes in technology. Computer security measures can however be beefed up by using anti-virus software, access control, firewalls and by employing qualified IT or IT-security staff. Added to these measures should be the adequate training of staff on computer security. As a result of all the factors militating against computer security of organizations, the tested hypothesis showed that the total eradication of computer crimes is not possible. It can however be reduced through public education, compliance using effective security technologies, having law enforcement agents equal in technical skill to computer criminals, and the establishment of a balanced standard for the prosecution of computer criminals.

## CONCLUSION

Based on the findings of this study, it can be concluded that computer crimes are being experienced by the Nigerian banking sector. These crimes are not harmless; they are causing banks financial loss which would ultimately have an adverse effect on the economy. Most banks have measures in place to manage the occurrence of computer crimes but based on the fact that technology advance on a daily basis, bank management should try to keep up with these advances in other to efficiently combat computer crimes and reduce them to the barest minimum.

## REFERENCES

Arellano, N. (2007). "Computer Crime: Top Threats in 2007". http://www.crime-research.org/articles/Computer-crime-Top-threats-in-2007/2, Accessed on 19/02/2010.

Computer Crime Research Center, (2005) on "Types of Computer Crimes", "Prevention of Computer Crimes in Banking", "Computer crime: internet banking perspective"

http://www.crime-research.org/news/, Accessed 19/02/2010.

Computer Security Institute. (1999) “Issues and Trends: 1999 CSI/FBI Computer Crime Survey” http://www.gosci.com/prelea990301.html, Accessed on 19/02/2010.

Denning, D. (2000) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy http://www.nautilus.org/info-policy/workshop/papers/denning. html, Accessed on 19/02/2010.

Gold, S. (2009) “BT Starts Switchboard Anti-Hacking Investigation” (Newsbytes) http://www.infowar.com/, Accessed on 19/02/2010.

Grabosky, P. N. (2000). “Computer Crime: A Criminological Overview” Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna.

Hundley, R. and Anderson, R. (1995) “Emerging Challenge: Security and Safety in Cyberspace”, IEEE Technology and Society Magazine, 14(4): 19-28.

Lovet, G. (2007). “How Cyber Crime operations work and why they make money” available at http://www.crime-research.org/analytics/2524/ (22.02.2007) Accessed on 16/01/2010.

Meier J.D., Mackman A., Dunner M., Vasireddy S., Escamilla R. and Murukan A. (2006) Improving Web Application Security: Threats & Countermeasures. http://msdn2.microsoft.com/en-us/library, Accessed on 16/01/2010.

Rathinasabapathy, G. (2005). “Cybermedicine: A Study on the Problems with Online Healthcare Information Resources”. In: Proceedings of the Annual Conference of Medical Library Association of India, NIMHANs, Bangalore.

TechWarehouse (2004) Types of Computer Crimes http://www.techiwarehouse. com/cms/engine. php, Accessed on 16/01/2010.