INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 3412 Cities in 173 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS AND SYSTEM RISK MANAGEMENT IN NIGERIAN BANKS

DR. DAFERIGHE, EMMANUEL EMEAKPONUZO
LECTURER, DEPARTMENT OF ACCOUNTING, FACULTY OF BUSINESS ADMINISTRATION, UNIVERSITY OF UYO, NIGERIA: & DIRECTOR
CENTRE FOR SOCIAL AND ENVIRONMENTAL ACCOUNTING RESEARCH (CSEAR)
NIGERIA

DR. UDIH, MONEY
LECTURER
DEPARTMENT OF GENERAL STUDIES & ENTREPRENEURSHIP
COLLEGE OF SCIENCE
FEDERAL UNIVERSITY OF PETROLEUM RESOURCES
EFFURUN (FUPRE)

ABSTRACT

The advent and adopted of Information Technology (IT) have improved performance in business and accounting processes in the organizations. However, the attendant risks associated with this cannot be denied. The main objective of this paper was to evaluate Computerized Accounting Information System (CAIS) and system risk management in the Nigerian banking sector. It was an empirical survey of commercial banks in four states; namely Akwa Ibom, Cross River, Delta and Rivers; in the south-south region of Nigeria using a questionnaire designed on a bipolar scale of five. It was revealed that the greatest risks associated with CAIS of banks in Nigeria are salami fraud, acts of nature, logic bombs and data diddling; and that the mostly adopted techniques and tools for management of CAIS risks are penetration testing, use of mitigation and recovery means, and malware scanners. It was also discovered that the greatest challenges faced by Nigerian banks in this respect are difficulty in obtaining physical evidence and witness cooperation, and difficulty in understanding the offender's method. The Chi-square statistical tool was used to test the hypothesis which revealed that there was significant relationship between techniques and tools adopted for system risk management and the challenges associated with CAIS. The strength of relationship between the variables was 89.6% as determined using Spearman's rank correlation coefficient .The paper therefore recommended that banks in Nigeria should install infrastructures such as Address Verification System (AVS), Interactive Voice Response (IVR), Internet Protocol (IP) address tracking systems and Intrusion Detection Systems (IDS). These will go a long way to managing the vulnerability associated with CAIS which will invariably enhance effectiveness and guarantee greater results.

KEYWORDS

Computerized accounting information system(CAIS), information technology, Nigerian banks, risks, system risks management.

INTRODUCTION

Information Technology (IT) has undoubtedly played a remarkable role in the business sector in recent times. The rapid change in IT; the wide spread of user-friendly systems and the great desire of organizations to acquire and implement up to date computerized systems and software have made computers much easier to be used and have enabled accounting tasks to be accomplished much faster and more accurate than hitherto. According to Wang, Ballou, Pazer and Tayi (1998), more and more organizations believe that quality information is critical to their success.

With rapid development of IT; Computerized Accounting Information Systems (CAIS) play an increasingly crucial role in the organizations regardless of their size. The world is moving rapidly to the point where it is possible to assert that everything depends on computer software (Edwards & Anderson, 1995). The exponential growth of technology; the increase in its capacity and accessibility and decrease in its cost; have brought about evolutionary changes in commerce, communication, entertainment and education. With this greater capacity, however, comes greater vulnerability. Information technology has begun to provide criminal opportunities of which olden day's criminal never dreamt. This advanced technology has also created significant risks related to ensuring the security and integrity of CAIS (Abu-Musa, 2005).

Apart from the advantages of the CAIS, several deadly deficiencies and threats in terms of the security and reliability of the accounting information system may emerge; which may be detrimental to the interest of the organization and even worse; may lead to the collapse of a company. The fundamental precept of information security is to support the organization against these threats and uncertainties posed by CAIS; hence, IT professionals must be able to help their organizations understand and manage these uncertainties.

System risk management plays a vital role in the mitigating these risks; as it helps in the understanding and responding to factors that may lead to failure in the confidentiality, integrity or reliability of CAIS. It is worthy of note that technology in many cases, has developed faster than the advancement in control practices and has not been combined with similar development in employees knowledge, skill, awareness and compliance.

Often time reports can be found in accounting and financial publications about computer related data errors, incorrect financial information, violation of internal control, theft, burglaries, spam, hacking, impersonation, sabotage and so on. Organizations should be aware of the potential security risks that might challenge their CAIS. The risks associated with CAIS are numerous owing to its vulnerability; not only in integral part of organization such as asset theft, artificial revenue information, expense manipulation, change of the CAIS illegally and so on; but also the external; such as hacking, spam, phishing and identity fraud.

Although considerable efforts have been made by practicing accountants and IT professionals to reduce the vulnerability of CAIS; it is argued that an increasing effort is still required (Abu-Musa, 2005). Today, not only computer whiz kids hack into computers, IT professionals have joined the league (Olasanmi, 2010). A new breed of white collar criminals has emerged and is infiltrating systems one way or the other. The introduction of the internet has heightened the threats of these crimes.

In 2005, the then Economic and Financial Crimes Commission (EFCC) Chairman in Nigeria; Malam Nuhu Ribadu stated that the Commission had confiscated at least 100 million United States Dollar (USD) from scammers and other defendants and by the time he was temporarily removed from office in 2008, the Commission had retrieved a total of 600 million USD in dubiously acquired funds. An anonymous survey by the EFCC recorded instances of electronic theft of up to 500 million USD (Tedeschi, 2003). According to Brey (2001), the internet has been used to gain illegal access to systems. Regrettably, 80% of these e-crimes remain practically undiscovered (Balogun & Obe, 2010).

According to Olasanmi (2010), estimating the incidence, prevalence, costs or some other measures of crimes related to computerized systems have posed some challenges as such crimes are not easily detected and even when detected, reports to the appropriate authorities are not always made due to the need of some organizations to protect some private information. It is in the face of these challenges that this paper seeks to:

(i) determine the different risks associated with CAIS in Nigerian banks;
(ii) appraise how these risks are managed by these banks; and

(iii) assess the challenges faced in the management of these risks.

The basic assumption for this paper is that there is no significant relationship between the techniques and tools adopted by Nigerian banks for system risk management and the challenges associated with CAIS.

LITERATURE REVIEW

In order to understand CAIS, it is pertinent to first review what an Accounting Information System (AIS) is. This will provide a proper perspective for appreciating what CAIS is all about.

THE ACCOUNTING INFORMATION SYSTEM

Accounting is a service function that seeks to provide the users with qualitative information; while AIS is an information system that is designed to make the accomplishment of the accounting function possible. Accounting Information System is a system of collection, storage and processing of financial and accounting data that is used by decision makers. According to Romney, Steinbart and Cushing (1997), AIS processes data and transactions to provide users with the information they need to plan, control and operate their businesses. The resultant reports can be used internally by management and externally by other interested parties such as investors, creditors and tax authorities. An AIS can be manual system or a computerized system; using computers. The components of AIS include; people, procedures and instructions, data, software applications, information technology infrastructure, and internal control and security measures.

THE COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS

Along with the improvement in the technology, information systems have been computerized. The result is that manual booking keeping systems have been replaced by computerized ones. According to Nash (1989), the revolution in the information system which started in the early 1950s when the first business computer became available is still in progress.

Companies now capture, process, store and transmit data with the help of the computers. Where data collection and processing were performed manually hitherto; on-line collection and processing of data are performed now by computer systems (Grabski & Marsh, 1994). This improvement in technology has enabled companies to collect, process and retrieve data quickly.

The CAIS though very useful and almost indispensible have some challenges. These include among others:

- computer systems are always at risk of being hacked, faced with power failure and virus attack with may result in lose of information;
- systems can be costly and they require constant updating and staff need to be trained to efficiently use the system;
- security issues are posed with a risk of computer fraud;
- human error is often not quickly identified, and records input need to be validated for accuracy;
- computerized accounting systems can be difficult to understand and if the systems are not specifically adapted to the business; it can cause havoc to the accounts;
- computerized accounting systems are dependent on machine and other software to work properly. If something goes wrong with the computer, access to the software is restricted and work cannot be done. Time and expenses are involved in solving the problem so as to get operations going.

There are many computer frauds and computer crimes exercised through CAIS owing to its vulnerability not only in the internal part of the organization such as asset theft, artificial revenue information, expense manipulation, change of the CAIS illegally and so on; but also the external such as hacking, spam, phishing, identity theft and so on.

The risks involved in CAIS include sabotage (physical damage to computer system), impersonation, phone phreaking, data diddling, hacking, salami fraud, logic bombs, extortion, spam amongst others.

SYSTEM RISK MANAGEMENT

Risk is the potential harm that may arise from some current process or from future event. Risk is present in every aspect of our life and different disciplines focus on risk as it applies to them. From the IT perspective, risk management is the process of understanding and responding to factors that may lead to a failure in confidentiality, integrity or availability of an information system.

Information Technology security risk is the harm to a process or the related information resulting from some purposely or accidental event that negatively impacts the process with the attendant adverse effect on the organization. Some of these threats to information systems include accidental disclosure, alteration of software and intentional alteration of data. Others are system configuration error, telecommunication malfunctioning/ interruption and vulnerabilities (weakness in system security procedures, design, implementation and control).

An understanding of risk and the application of risk assessment methodology is essential to efficiently and effectively creating secured computing environment. All organizations operating a CAIS are exposed to uncertainties; some of which impact negatively on the organization. Therefore, the fundamental objective of information security is to support the mission of the organization.

Managing risks and uncertainties is not an easy task; for there is an ever-changing landscape of threats and vulnerabilities. Hence, IT security professionals must be able to help management of their organizations understand and manage these risks. Loch, Houston and Warkentin (1992) found that natural disaster, employee accidental actions (inadequate control over media) and unauthorized access to CAIS by hackers ranked among the top security threats. This goes to say that the greater risks are from inside the organization. Davis (1996); Ryan and Bordoloi (1997) corroborate this claim.

On the nature of the accounting systems and security in use Henry (1997) states that 80.3% of companies secured their accounting systems using passwords but only 42.7% utilized protection from viruses. He further stated that less than 40% have measures for physical security and authorization for changes to the system and sadly less than that figure use encryption for their accounting data. This calls for concern considering the number of companies utilizing some form of hardware and software or the other.

Hood and Yang (1998) in their comparative study of the impact of banking information system in China and UK found that management was aware of security risk but they have not taken enough action to reduce the risks and losses owing largely to lack of financial and human resources. On understanding how organizations are addressing their IT risks; Hermanson, Hall and Irancevich (2000) study revealed that internal auditors focus primarily on traditional IT risks and controls; such as asset safeguarding, application processing and data integrity, privacy and security.

Abu-Musa (2005) investigated the security risks associated with CAIS in the Egyptian banking sector. The study revealed that accidental entry of bad data by employees, introduction of computer viruses to the system, employees sharing of passwords; and misdirecting information to people not entitled to receive them were the most perceived significant security threats to CAIS in the Egyptian banking sector.

WHY IS IT IMPORTANT TO MANAGE RISK?

The principal reason for managing risk in an organization is to protect the mission and assets of the organization. The first step in risk management is an understanding of the risk. An understanding of the specific risk to a system allows the system owner to protect the information system. Different risk management schemes offer different methodologies for identifying vulnerabilities and assessing risk. Assessing risk is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise.

There is great need to make detailed preparations to withstand and recover from a wide range of unwanted cyber events; both accidental and deliberate. There are significant and growing risks of localized misery and loss as a result of compromise of computer and telecommunication services. Risks management approaches are most useful when there is a reasonable level of available reliable data about the risk being considered where there are probabilities and clearly definable potential financial losses.

According to Cashell (2004), the response usually is to adopt a three matrix of high, medium and low levels of probability, and another three level matrix of impact; which allows for some of the disciplines of risk management to be adopted without the need for precise financial calculation. Some remedies to system risk are system design which integrates security features into the initial requirement engineering, detective and preventive measures which provide opportunity to stop breach of basic routine security; this is the first essential step in the more complex series of actions necessary to achieve an event of significant information security technologies.

When preventive and detective methods fail, the emphasis switches to mitigation and recovery factors; as a function of the structure of the organization that is affected and to determine if there is a well tested contingency plan. Thompson (1989) identified a number of challenges of curbing risks associated with CAIS. He listed some factors to include:

- a large proportion of computer related crimes are 'insider jobs';
- e-crimes are generally of low visibility and therefore difficult to detect;
- once the crime has been detected; discovery and understanding the method used by the offenders in a technologically complex crime can be difficult;
- the ability to obtain physical evidence is generally more difficult than in other commercial crimes;
- computerized information; which is of evidentiary value can easily be altered or destroyed; often leaving no trace of tempering; and
- issues involving the admissibility of evidence in court is further complicated in the computerized environment.

METHODOLOGY

The area of study was four states of the south-south region of Nigeria; namely Akwa Ibom, Cross River, Delta and Rivers; and the main focus was on the risks associated with CAIS faced by banks in Nigeria. The universe of the study was all commercial banks in Nigeria and period of study was 2012. In the survey, a total of 200 copies of questionnaire were administered to IT representatives in various commercial banks across the four states. The questions were on bipolar scale of five. Responses were ranked and analyzed. The chi-square (χ^2) statistical tool is used to test the hypothesis at 5% level of significance while the strength of association is evaluated using the Spearman's rank correlation coefficient. The purpose is to establish the pattern of association between CAIS and risk and evaluate efforts in managing the risks.

DATA PRESENTATION AND RESULTS OF ANALYSIS

TABLE 1: FREQUENCY OF RISKS ASSOCIATED WITH CAIS OF BANKS

S/N	RISK	FREQUENCY	PERCENTAGE	RANKING
1	sabotage	114	57	19
2	impersonation	107	54	22
3	credit card fraud	151	75	5
4	phone phreaking	136	68	14
5	data diddling	158	79	3
6	salami fraud	172	86	1
7	logic bombs	157	79	4
8	extortion	107	54	22
9	Spam	150	75	6
10	denial of service	142	71	12
11	hacking	150	75	6
12	notorious worms & viruses	129	65	15
13	trojan horse	107	54	22
14	Accidental disclosure	143	72	10
15	Bandwidth interference	114	57	19
16	Alteration of software	142	71	12
17	Electrical interference	143	72	10
18	System configuration error	150	75	6
19	Telecommunication malfunction	121	61	18
20	Acts of nature:thunder, earthquake	165	83	2
21	Phishing	122	61	16
22	Keylogger	150	75	6
23	Root-kit	114	57	19
24	System overload	122	61	16

Source: Field survey 2012

Table 1 shows that the greatest risks associated with CAIS of banks in Nigeria are salami fraud (86%), acts of nature; such as thunder (83%), logic bombs (79%) and data diddling (79%). These risks cause more problems to Nigerian banks as their level of occurrence is very high. The lowest risks are impersonation, extortion and Trojan horse (all at 54%).

TABLE 2: DEGREE OF ADOPTION OF TECHNIQUES AND TOOLS FOR MANAGEMENT OF RISKS ASSOCIATED WITH CAIS

TECHNIQUES FOR MGMT OF RISK	FREQUENCY	PERCENTAGE	RANKING
1. Access control facilities(passwood & codes)	170	85	7
2. Virus scanners	171	86	5
3. Malware scanners	192	96	3
4. Penetration testing	193	97	1
5. Electronic data processing (EDP) audit	150	75	11
6.Use of failsafe systems	136	68	12
7. Use of cryptography	157	79	9
8. Load balancing	186	93	4
9.Use of input validation routines e.g validity checks, sign checks etc	170	85	7
10. Use of tripwires, honey pot lures & anomaly detection system	157	79	9
11. Use of infrastructure such as address verification system (AVS), interactive voice response (IVR) etc	65	33	13
12. Use of video surveillance systems	171	86	5
13. Use of mitigation and recovery means	193	97	1

Source: Field survey 2012

Table 2 shows the level of adoption of various techniques and tools for management of risks associated with CAIS. The mostly employed techniques are Penetration testing (97%), Use of mitigation and recovery means (97%) and Malware scanners (96%). On the other hand the least employed is the use of infrastructure such as Address Verification System (AVS) and Interactive Voice Response (IVR) (33% respectively).

TABLE 3: CHALLENGES FACED IN THE MANAGEMENT OF RISKS ASSOCIATED WITH CAIS

CHALLENGES FACED IN MGMT OF RISKS IN CAIS	FREQUENCY	PERCENTAGE	RANKING
1. Low visibility & difficulty in crime detection	134	67	11
2. International jurisdictional boundaries	130	65	12
3. Insider job	142	71	9
4. Difficulty in discovery & understanding the offenders method in technologically complex computer	171	86	3
5. Difficulty in obtaining physical evidence	172	86	1
6. Complications in admissibility of evidence in court especially in the computerized environment	128	64	13
7. Difficulty in carrying out investigations	157	79	4
8. Apathy of some countries to E-crime	157	79	4
9. Obtaining witness cooperation	172	86	1
10.Identifying suspects	157	79	4
11. Problem of encryption	141	72	9
12.Locating and securing relevant materials	143	72	8
13. Difficulty in bringing the offenders to trial	157	79	4

Source: Field survey 2012

Table 3 shows the extent of challenges faced by Nigerian banks in the management of risks associated with CAIS. The greatest challenges are Difficulty in obtaining physical evidence, obtaining witness cooperation and difficulty in discovery and understanding the offender's method which were 86% respectively; while complications in admissibility of evidence in court is the least of all the identified challenges (64%).

TESTING OF HYPOTHESIS

The following hypothesis was tested:

H_o: There is no significant relationship between the techniques and tools adopted by Nigerian banks for system risk management and the challenges associated with CAIS.

TABLE 4: DEGREE OF ADOPTION OF TECHNIQUES AND TOOLS AND THE FREQUENCY OF CHALLENGES FACED BY MANAGEMENT

	TECHNIQUES & TOOLS	CHALLENGES	TOTAL
1.	170	134	304
2.	171	130	301
3.	192	142	334
4.	193	171	364
5.	150	172	322
6.	136	128	264
7.	157	157	314
8.	186	157	343
9.	170	172	342
10.	157	157	314
11.	65	141	206
12.	171	143	314
13.	193	157	350
TOTAL	2111	1961	4072

Source: Field survey 2012

$$\chi^2 = \frac{(o-e)^2}{e}$$

where

χ^2= chi-square

o = observed frequency

e = expected frequency

The chi-square was computed to test the hypothesis at 5% level of significance. The calculated χ^2_{cal} =20.950 which is greater than the tabulated $\chi^2_{tab\ 0.95(12)}$= 5.22603. Hence, the null hypothesis is rejected. Therefore there is significant relationship between the techniques and tools adopted by Nigerian banks for system risk management and the challenges associated with CAIS.

TABLE 5: EVALUATION OF THE DEGREE OF RELATIONSHIP BETWEEN TECHNIQUES AND TOOLS FOR SYSTEM RISK MANAGEMENT AND THE CHALLENGES FACED BY MANAGEMENT

ITEMS	RANK OF TECHIQUES & TOOLS	RANK OF CHALLENGES	D	D^2
1.	7	11	-4	16
2.	5	12	-7	49
3.	3	9	-6	36
4.	1	3	-2	4
5.	11	1	10	100
6.	12	13	-1	1
7.	9	4	5	25
8.	4	4	0	0
9.	7	1	6	36
10.	9	4	5	25
11.	13	9	4	16
12.	5	8	-3	9
13.	1	4	-3	9

$r = 1 - 6 \sum D^2$

$N^3 - N$

Where

r = coefficient of rank correlation

N = number of observations

$\sum D^2$ = summation of square of deviation

$r = 1 - 6(326)$

$133 - 13$

r = 0.896

The result showed that there is a significantly high positive correlation of 89.6% between the techniques and tools adopted by Nigerian banks and the challenges associated with CAIS.

DISCUSSION OF FINDINGS

The paper revealed so many risks summing up to 24 that are associated with CAIS but the ones affecting the banks at a very high rate and serving as a menace to the CAIS as a whole include acts of nature, data diddling, salami fraud and logic bombs. Other risks are spam, hacking, notorious worms/viruses, accidental disclosure, alteration of software, electrical interference, system configuration error, telecommunication malfunction, phishing and system overload.

The paper also revealed the mostly adopted techniques and tools intensively employed by Nigerian banks in managing these risks as penetration testing; such as validity checks, sign checks and completion checks, use of mitigation and recovery means and malware scanners. Other methods include the use of access control facilities such as passwords and biometrics and the use of video surveillance system.

It was revealed that there were other methods that have been either totally neglected or slightly implemented by banks in Nigeria and this leaves CAIS at a very vulnerable state. These methods include Electronic Data Processing (EDP) auditing, use of failsafe systems and use of cryptography. Others are use of tripwires, honey pot lures and anomaly detection system such as Address Verification System (AVS) and Interactive Voice Response (IVR).

The paper revealed that there is significantly high positive correlation of 89.6% between the techniques and tools adopted by Nigerian banks for system risk management and the challenges associated with CAIS. These tools and methods adopted by banks in Nigeria are not without challenges and limitations. The greatest of these are identified as insider job, difficulty in discovery and understanding the offender's method in a technologically complex computer environment, difficulty in obtaining physical evidence while complications in admissibility of evidence in court is identified as the least challenging. Other challenges are difficulty in carrying out investigations and obtaining witness cooperation, problem of encryption, locating and securing relevant materials and difficulty in bringing the offender to trial. Hence, there is the need for more innovations by banks in Nigeria in tackling the challenges of CAIS.

CONCLUSION AND RECOMMENDATIONS

The paper concludes that the role of information technology in accounting is indispensible despite its vulnerabilities. It is observed that if the risks associated with CAIS are not properly managed it will adversely affect the main function of accounting. In spite of efforts made to curb these risks, there are challenges faced and banks in Nigeria are not adequately protected from these risks. Therefore, the paper proffers the following recommendations:

1. Banks should employ professional ICT persons to protect their CAIS from hackers and malicious programmers and to track down offenders.
2. Banks in Nigeria that do not have infrastructures such as Address Verification System (AVS) and Interactive Voice Response (IVR) terminals should install and use them. They should also employ Internet Protocol (IP) address tracking systems and Intrusion Detection Systems (IDS).
3. There should be scheduled programs and IT forum organized for staff of the banks and E-crime safety rules should be applied.
4. Relevant ICT security agencies should be constituted and empowered by government. The use of biometrics, firewalls and other access control facilities should be enhanced.
5. Security classification of data should be established and different access restrictions for each classification should be implemented in all the banks.
6. Security controls check lists should be used by banks to help internal auditors in identifying and correcting their CAIS security exposures through evaluating the security controls. Auditors should expand their knowledge of new business-oriented information systems; as such knowledge would facilitate the development of more effective audit approaches.
7. Finally, banks should adopt a balanced approach to security controls which places equal emphasis on technical, formal and informal interventions against their computerized systems in order to minimize losses through computer fraud. Mandatory vacations of employees should be considered and personnel policies including the rotation of duties should be enhanced.

REFERENCES

1. Abu-Musa, A. (2001). "Evaluating the security of computerized Accounting Information System: An empirical study on Egyptian banking industry." Unpublished Ph. D Thesis, Aberdeen University, UK.
2. Balogun, V. F. & Obe, O.O. (2010). "E-crime in Nigeria: Trends, tricks and treatment." *Pacific Journal of Science and Technology*, vol. 11(1) pp343-355.
3. Brey, P. (2001). Disclosure computer ethics, In Spinello, R.A. and Tavani, H.T. (ed.s). *Readings in Cyber Ethics*, Sudbury MA: Jones and Barlett.
4. Cashell,R. (2004). The economic impact of cyber attacks CRS report for Congress. Centre for the protection of National infrastructure. What we do. www. cpnigov.uk.about/what we do. aspx. Viewed on 12 November, 2012.
5. Davis, C. E. (1996). "Perceived security threats to today's accounting information systems: A survey of CAIS." *Information in Audit and Control*. pp38-41.
6. Edwards, R. & Anderson, R. (1995). "Emerging challenge: Security and safety in cyberspace." *IEEE Technology and Society magazine*, 14(14) pp19-28.
7. Grabski, S.V. & Marsh, R. J. (1994). "Integrating accounting manufacturing information systems: An AB and REA-based approach." *Journal of Information Systems*, pp61-80.
8. Henry, L. (1997). "A study of the nature and security of accounting information systems: The case of Hampton roads. Virgina:" *Mid-Atlantic Journal of Business*, pp171-189.
9. Hermanson, D.R., Hill, M.C. & Ivancevich, D.M. (2000). "Information technology-related activities of internal auditors." *Journal of Information Systems*, 14(1) pp39-53.
10. Hood, K.L. & Yang, J. (1998). "Impact of Banking Information System security on banking in China: The case of large state-owned banks in Shenzhen Economic special zone: An introduction." *Journal of Global Information Management,* pp5-15.
11. Loch, K. D., Houston, H.C. & Warkentin. M. E. (1992). "Threats to information systems: Today's reality, yesterday's understanding." *MIS Quarterly*, 16(2) pp 173-186.
12. Nash, J.F. (1989). *Accounting information system*. 2nd ed. PWS: Kent Publishing Company.
13. Olasanmi, O.O (2010). Computer crimes and counter measures in the Nigerian banking sector. A paper presented on National workshop on computer crime.
14. Romney, M.B., Steinbart, P.J. & Cushing, B. E. (1997). *Accounting information systems*. 7th ed. Reading, MA: Addison-Wesley.
15. Ryan, S. D. & Bordoloi, B. (1997). "Evaluating security threats in mainframe and client/server environments." *Information and Management*, Jan. 32 pp137-146.

16. Tedeschi, B. (2003). Cybercrime, they just don't mention it: The Age. http//:www.theage.com.au/articles/2003/01/30/1043804447447.html. Viewed on 12 November, 2012.
17. Thompson, D. (1989). "Police powers - where's the evidence?" Proceeding of Australian computer abuse inaugural conference.
18. Wang, R.I., Ballou, D.P., Pazer, H. & Tayi, G. K. (1998). "Modeling information manufacturing systems to determine information product quality." *Management Science*, 44(4) pp462-484.

APPENDIX

TABLE A

S/N	RISK	ALWAYS	OCCASIONALLY	NO IDEA	RARELY	NOT AT ALL	TOTAL
1	sabotage	57	57	43	14	29	200
2	impersonation	71	36	29	43	21	200
3	credit card fraud	86	65	14	14	21	200
4	phone phreaking	57	79	21	36	7	200
5	data diddling	101	57	14	21	7	200
6	salami fraud	79	93	14	14	0	200
7	logic bombs	100	57	14	29	0	200
8	extortion	57	50	36	14	43	200
9	spam	79	71	36	14	0	200
10	denial of service	57	85	29	29	0	200
11	hacking	93	57	22	14	14	200
12	notorious worms & viruses	100	29	29	29	13	200
13	trojan horse	29	78	36	14	43	200
14	Accidental disclosure	79	64	36	7	14	200
15	Bandwidth interference	43	71	36	36	14	200
16	Alteration of software	85	57	29	29	0	200
17	Electrical interference	93	50	21	36	0	200
18	System configuration error	79	71	14	29	7	200
19	Telecommunication malfunction	71	50	43	29	7	200
20	Acts of nature:thunder, earthquake	65	100	21	7	7	200
21	Phishing	93	29	36	21	21	200
22	Keylogger	36	114	14	22	14	200
23	Root-kit	29	85	50	7	29	200
24	System overload	79	43	36	14	28	200

TABLE B

TECHNIQUES FOR MGMT OF RISK	STRICTLY EMPLOYED	SLIGHTLY EMPLOYED	NO IDEA	RARELY EMPLOYED	NEVER EMPLOYED	TOTAL
1. Access control facilities(passwood & codes)	121	57	0	22	0	200
2. Virus scanners	128	43	0	29	0	200
3. Malware scanners	121	71	0	8	0	200
4. Penetration testing	114	79	0	7	0	200
5. Electronic data processing (EDP) audit	65	85	0	43	7	200
6.Use of failsafe systems	65	71	0	57	7	200
7. Use of cryptography	79	78	0	36	7	200
8. Load balancing	122	64	0	7	7	200
9.Use of input validation routines e.g validity checks, sign checks etc	85	85	0	30	0	200
10. Use of tripwires, honey pot lures & anomaly detection system	43	114	0	29	14	200
11. Use of infrastructure such as address verification system (AVS), interactive voice response (IVR) etc	29	36	0	85	50	200
12. Use of video surveillance systems	142	29	0	29	0	200
13. Use of mitigation and recovery means	93	100	0	7	0	200

TABLE C

CHALLENGES FACED IN MGMT OF RISKS IN CAIS	HIGH EXTENT	MEDIUM EXTENT	NO IDEA	LOW EXTENT	NOT AT ALL	TOTAL
1. Low visibility & difficulty in crime detection	67	67	14	43	9	200
2. International jurisdictional boundaries	65	65	21	43	8	200
3. Insider job	121	21	15	29	14	200
4. Difficulty in discovery & understanding the offenders method in technologically complex computer	100	71	7	15	7	200
5. Difficulty in obtaining physical evidence	121	51	7	14	7	200
6. Complications in admissibility of evidence in court especially in the computerized environment	71	57	15	43	14	200
7. Difficulty in carrying out investigations	114	43	14	21	8	200
8. Apathy of some countries to E-crime	100	57	14	15	14	200
9. Obtaining witness cooperation	107	65	7	14	7	200
10.Identifying suspects	136	21	14	29	0	200
11. Problem of encryption	114	29	14	36	7	200
12.Locating and securing relevant materials	129	14	7	43	7	200
13. Difficulty in bringing the offenders to trial	114	43	7	36	0	200

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals