IRMM
INTERNATIONAL REVIEW OF MANAGEMENT AND MARKETING
EJ EconJournals
ISSN: 2146-4405

International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2017, 7(2), 340-346.

EJ EconJournals

Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness

Stephen A. Ojeka[1]*, Egbide Ben-Caleb[2], Edara-Obong Inyang Ekpe[3]

[1]Department of Accounting, Covenant University, Ota, Ogun State, Nigeria, [2]Department of Accounting, Covenant University, Ota, Ogun State, Nigeria, [3]Department of Accounting, Covenant University, Ota, Ogun State, Nigeria.
*Email: stephen.ojeka@covenantuniversity.edu.ng

ABSTRACT

This study appraises the relationship that exists between cyber security and audit committee effectiveness using audit committee independence, audit committee technological expertise and audit committee financial expertise characteristics as independent variables. The variable used to measure the dependent variable is cyber security compliance. 13 banks listed on the Nigerian stock exchange were selected. Empirical analysis was carried out using product moment correlation and ordinary least square regression analysis methods. The result showed that audit committee characteristics as measure by independence, financial expertise and technological expertise all have non-significant negative relationship to cyber security in the Nigerian banking sector. The implication is that, the audit committee as presently constituted in Nigeria would be unable to provide controls and oversight functions over cyber security in the banking sector which is the most sensitive sector in the economy. It was therefore recommended that the composition of the audit committee in Nigeria should be worked on to deliberately incorporate needed technological and financial experts that can ask probing questions and offer their wealth of experience in safeguarding the shareholders wealth and lastly, the committee members should be seen to be independent.

Keywords: Audit Committee, Banking Sector, Cyber Security, Financial Expertise, Independence, Nigeria
JEL Classification: M4

1. INTRODUCTION

Technological development has improved daily life in areas such as online banking and shopping. The digital domain has become an important factor in the world and information and communication technology has proved to be a very vital factor in productivity, growth and innovation (Rosewarne, 2014). In recent years, the world has greatly developed technologically and the development has also affected accounting practices (Ernst and Young, 2013).

However, the growth of the information and communication technology environment is accompanied by new and serious threats. Cyber-attacks now have the ability to greatly harm the society in new and critical ways. Online fraud and cyber-attacks are just a few examples of computer related crimes that are committed on an extremely large scale every day (Gercke, 2006). For a long time, cyber-crime has tarnished Nigerian international reputation and greatly discouraged foreign investors. The phenomenal rise of mobile communication and the drive from the Central Bank of Nigeria towards a cashless economy has contributed to the growth of cyber-crime. Odunfa (2014) opines that the financial damages incurred by cyber-attacks are reported to be very high and rapidly increasing. According to report by Nigeria inter-banks settlement systems, Nigerian banks have lost NGN 159 billion between 2000 and 2013 to cyber-crime and according to Nigeria-based information and communications technology company New Horizons Limited, NGN 413 billion (USD 2.5 billion) is being lost annually to cyber-crime. Although these financial cost can be measured, cost in human misery and tragedy is incalculable and now it is costing more than physical crime (Ali et al., 2014). The need to improve cyber security and protect critical and delicate information is extremely necessary for every nation's security and economic well-being.

These developments have highlighted the need to protect stakeholder's interest and audit committee significance. KPMG (2013) states that most audit committee members are financially shrewd to a certain degree but lack an in-depth knowledge of technological issues. This makes the audit committee members rely

greatly on the technology officials within the company to provide them with whatever perspective and opinion on information technology. In as much as these technology officials can provide data, it can prove to be difficult to convert the data into meaningful information that could possibly be useful to the board members and the audit committee in helping to give a better understanding of the possible risk the entity is facing. Also, the audit committee may not know how to evaluate the information they receive and will possibly not know the right follow-up questions to ask. The uncertainty can lead to hesitation and if not properly addressed, inaction can damage a company's reputation and possibly brand, disrupt business continuity and possibly lead to a great deal of financial and legal complications (Ernst and Young, 2013).

The audit committee has oversight responsibility on the activities of the board concerning the issue of cyber security to protect the best interest of the stakeholder (Adeyemi et al., 2012). There is the need for the audit committee to gain better information about the company's processes, and the information should be used as an advantage to understand whether management has put the right people, processes and generally the best possible strategy. The action plan of the audit committee will depend greatly on the maturity level of the company to manage security risks and will require more time and attention in particular sectors. Various studies have looked at the audit committee responsibility on cyber security (Ernst and Young, 2013; Lewis, 2013), their influence on the board for better performance, the economic impact of cyber-crime and cyber espionage. Ernst and Young (2013) found that an audit committee that will influence the board of directors on cyber risk and cyber security must possess certain attributes such as financial expertise, technological expertise, independence, leadership, commitment and the capacity to act.

Recently, cybercrime has turned into a growing threat to all companies worldwide and there is a need to address the issue for the protection of the company and their stakeholder. The effect of the breach on financial performance ultimately reduced earnings per share and overall market value of the affected companies (Ernst and Young, 2013). As a result of cyber-attacks, public trust and investors' confidence has been reduced towards companies, their directors, managers and auditors. The main objective of this research is to look into the activities and oversight function of the audit committee concerning the growing issue of cybercrime and the cyber security procedures being adopted by board of directors to tackle the growing threat to the Nigerian banking sector. Specificall , the study is to ascertain the relationship between audit committee independence (ACIND) and cyber security in Nigerian banks; and to examine the influ nce of audit committee technological expertise (ACTECH EX) and audit committee financial expertise (ACFIN EX) on cyber security in Nigerian banks.

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1. The Place of Audit Committee in Cyber Security in Nigerian Banks

The genesis of audit committees as part of corporate governance structure is rooted in the reactions to the abuse of power by corporate management as a result of financial scandals, manipulation of policies and misstatements of accounts (Kalber and Fogarty, 1998). Although fin ncial reporting and internal control risk continue to be top priority with regulatory compliance issues, bank audit committee attention continues to broaden considerably. The most recent issue vying for audit committee attention is technology concerns - particularly issues involving cyber security risks, growth through mobile banking applications, and upgrading information technology are gaining high profile The audit committee, aside from focusing on their crowded agenda, there is a broader concern about having the needed expertise to oversee management activities concerning cyber security. It is the duty of the audit committee to collaborate with management to increase efforts about threat awareness, timely discovery of incidents, risk assessments, and closer coordination with regulators about how cyber security risks are being identifie and managed.

The audit committee is a standing committee of the board of directors established to assist the board in fulfilling its oversight responsibilities relating to the accounting and financial reporting policies and practices, compliance programmes, internal controls and general compliance with applicable laws and regulations. Cyber security for financial institutions such as banks in Nigeria has been grossly affected by various factors involving the audit committee, some of which include independence, financial expertise and advancement of cyber security of the audit committee. The independence of the audit committee is to ensure that management is held accountable to shareholders (Adeyemi et al., 2012). The code of corporate governance states that the majority of audit committee member must be independent and the chairman should be an independent non-executive director. It is posited that the more independent the audit committee, the higher the degree of oversight and the more likely that members act objectively in evaluating the propensity of the company internal control and reporting practices.

Internet cyber criminals keep perfecting their fraud methods, leading to losses adding up to billions of naira yearly. To this end, there is a need for the audit committee to gain technological expertise as the crime artist constantly get more powers and better technical facilities to carry out the act. For the best interest of banks, it is necessary for the audit committee to gain technological expertise so as to keep with the growing trend of the global community. With respect to financial expertise on cyber security, Song and Windram (2000), opine that a high degree of financia literacy is necessary for an audit committee to effectively oversee a company's financial control and reporting. The role of an audit committee in overseeing accountability of the management covers a wide scope to include the overall process of risk management. This requires the audit committee to have accounting knowledge in order to acquire an in-depth understanding of financial implications of cybercrime. Financial literacy can reduce fraud in corporate financial reporting. A formal recognition of this requirement was recently made in the U.S. with the passing of the Sarbanes-Oxley Act (2002) which requires each public listed company to disclose whether or not it has a financial expert in the audit committee.

2.2. ACIND and Cyber Security

It is an essential factor for an audit committee to ensure that management is held accountable to shareholders (Adeyemi et al., 2012). The Code of Corporate Governance states that the majority of audit committee member must be independent and the chairman should be an independent non-executive director. It enhances the effectiveness of monitoring functions. It is posited that the more independent the audit committee, the higher the degree of oversight and the more likely that members act objectively in evaluating the propensity of the company internal control and reporting practices. This indicates that an independent audit committee is able to help companies sustain the continuity of business although when they are faced with financial difficult es, they are expected to propose certain action plans to mitigate the problem. An independent audit committee is highly useful to both the company and its shareholders. This independence will cause the board to work effectively on their respective duties.

2.3. ACTECH EX and Cyber Security

Internet cyber criminals keep perfecting their fraud methods, leading to losses adding up to billions of naira yearly. Therefore, specialized departments and structures are created to combat this type of crime. The audit committee has risk management duties to its stakeholders and due to the complexity of the cyber world, there is a need for the audit committee to gain technological expertise as the crime artist constantly get more powers and better technical facilities to carry out the act. For the best interest of banks, it is necessary for the audit committee to gain technological expertise as well to be able to keep with the growing trend of the global community.

2.4. ACFIN EX and Cyber Security

Song and Windram (2000) maintained that a high degree of financial literacy is necessary for an audit committee to effectively oversee a company's financial control and reporting. The role of an audit committee in overseeing accountability of the management covers a wide scope to include the overall process of risk management. This requires the audit committee to have accounting knowledge in order to acquire an in-depth understanding of fi ancial implications of cybercrime on the banks performance, share price, and other aspects that could affect the banks reputation or possibly lead to financial complication. The need to comprehend the overall financial and non-financial contents of corporate reports is greater considering that business activities are advancing beyond minor accounting practices and therefore, there is a need for presenting technically advanced financial reporting contents to keep stakeholders updated on both financial and non-financial activities. Financial literacy can reduce fraud in corporate fin ncial reporting. A formal recognition of this requirement was recently made in the U.S. with the passing of the Sarbanes-Oxley Act (2002) which requires each public listed company to disclose whether or not it has a financial expert in the audit committee.

2.5. Audit Committee Size (ACSIZE) and Cyber Security

The stock exchange of various countries requires that the audit committee of their listed companies be made up of at least three members (Al-Sa'eed and Al-Mahamid, 2011). Research suggests that a large audit committee tends to enhance the audit committee's status and power within the organization (Kalbers and Forgarty, 1993), to receive more resources, and to lower the cost of debt financing (Anderson et al., 2004). It is therefore expected that a larger audit committee is more likely to have effective control and also possess effectual influence because increased resources and enhanced status in the bank will make an audit committee to be more effective in fulfilling its core monitoring role in the organization. However, Yermack (1996) found that a board with a smaller size is related to a higher quality of monitoring. The study also showed that a smaller audit committee can easily forge the CEO to be more disciplined in cases of poor performance and also they can easily exchange information and relate efficiently within their members but in support of the former, a large audit committee may be more efficient in spotting problems in financial reporting.

2.6. Routine Updates on Risk and Advancement in Cyber Security

There is a need for bank audit committee to seek routine updates to the growing risk of cybercrime. As a result of the fact that cybercrime is a developing and fast changing risk as hackers create new software spamming back doors every day, there is a need for the audit committee to also stay updated on the risk. An anti-cybercrime strategy should be an integral element of cyber security strategy. Anti-cybercrime strategies developed in industrialized countries could be introduced in developing countries especially in Nigeria, offering advantages of reduced cost and time for development. The implementation of existing strategies could enable developing countries to benefit from existing insights and experience.

2.7. Audit Committee Effectiveness on Cyber Security

Audit committee is a corporate governance mechanism and effectiveness in financial reporting processes has been a cause of concern to the regulators and investors. Given the number of high profile fraud cases experienced in previous years in cases such as Enron, WorldCom, Parmalat, the consequence of these high profi e frauds have led to investors lack of confidence in financial reports and activities of companies (García-Sanchez, Jose and García -Rubio, 2012). Over the past years, the audit committee has been greatly criticized for not being effective enough to in ensuring that external auditors are independent so as to issue effective financial reports (Levitt, 2006b). Due to this criticism, regulators have intensified the watch over the activities of the committee. The code of corporate governance for banks in Nigeria requires the audit committee members to possess financial and accounting knowledge and also have a high level of independence. Due to the change in the nature of financial activities technological expertise can also be added to necessary knowledge needed by the audit committee members.

Lee and Stone cited in Mohuiddin and Karbhari (2010) noted that actual effectiveness is hard to observe. This then makes it a vague concept that can be approached in various ways. Various literatures have described audit committee's effectiveness as being able to carry out oversight functions (Raghunandan, Read and Rama, et al., 2001). Multiple studies have used its duties to

define its effectiveness (Mohuiddin and Karbhari, 2010). Kalber and Forgatry (1993) defined audit committee effectiveness as the competency with which the audit committee carries out its specified oversight responsibility. Also, DeZoort et al. (2002) defined and effective audit committee as one that has qualified members with the authority and resources to protect shareholders interest by ensuring reliable internal controls, risk management and financial reporting through its diligent oversight e forts.

Due to the fact that the audit committee is a sub-unit (committee) of the board of directors; various literature has put forth arguments that the effectiveness of the audit committee of one company cannot be assessed by just comparing it to the audit committee of other companies (Mohuiddin and Karbhari, 2010). Other studies have related audit committee effectiveness to its characteristics such as size, independence, expertise, and frequency of meeting. This can be further identified through four various components as identifie by DeZoort et al. (2002) which are; composition (independence and expertise of the members), authority (responsibility and influence), resources (size and access to government parties) and diligence (incentives, motivation and perseverance). In contrast to this, Wu (2012) had a suggestion that if effectiveness represents an ability to accomplish, then the effectiveness of the audit committee should be explained as ability and not as an association between the characteristics and output of an audit committee.

Rainsbury et al. (2008) found membership of audit committee as one of the key factors to improve audit committees effectiveness. Mohuidin and Karbhari (2010) posited that audit committees effectiveness depends mainly on how successfully they can carry out its roles and objectives no matter how they are composed.

The above and prior findings with regard to cyber security and audit committee effectiveness in Nigerian banks lead to the following hypotheses:

Hypotheses statement:
H_1: There is no significant relationship between ACIND and cyber security in the Nigerian banking sector.

H_2: ACTECH EX has no significant impact on cyber security of the Nigerian banking sector.

H_3: ACFIN EX has no significant impact on cyber security of the Nigerian banking sector.

3. RESEARCH METHODS

This study adopted a survey research design method to guarantee that the researchers reach a larger population; and aimed at establishing a relationship between ACIND and cyber security in the Nigerian banking sector. The secondary method of data collection for both quantitative and qualitative analysis was also adopted to gather information from the 21 listed banks on the Nigerian stock exchange for the year 2014 that constitute the population of study. In obtaining the sample technique for this study, a judgmental sampling technique was used in order to ensure representativeness from the listed banks. The researcher acknowledged the possibility of inconsistencies in the analysis and result, but according to Kyereoah-Coleman (2007) the differences that occur are very small. A sample size of 21 listed banks was selected based on the availability and accessibility of the audit committee report of the chosen companies. For the purpose of data analysis, a product moment correlation and ordinary least square regression analysis, based on computer programs known as Microsoft Office Excel 2010 and S ATA 11, were used.

3.1. Model Specificatio

For the purpose of measuring the relationship between dependent and independent variables, a mathematical model is hereby specified

$$Y=\beta_0+\beta X_1+\varepsilon \quad (1)$$

Where,
Y=Cyber security (dependent variable)
X=Audit committee effectiveness (independent variable)
β=Coefficien
ε=Error term

Equation 1 can be clearly defined as

Cyber security=f (audit committee effectiveness)+c (2)

Hence, the equation below is formulated with the inclusion of control variables (ACSIZE). This is to enhance better predictability of the relationship existing between the two constructs (audit committee effectiveness and cyber security).

CSCom=Audit committee independence+audit committee technological expertise+audit committee financial expertise+audit committee size (3a)

The above can be deduced to;

$$CSCom=ACInd+ACTech\ Ex+ACFin\ Ex+ACS \quad (4a)$$

Based on regression, the model specification is

$$CSCom=\beta_0+\beta_1 AInd_{it}+\beta_2 ACTech\ Ex_{it}+\beta_3 ACFinEx_{it}+\beta_4 ACS_{it}+\varepsilon_{it} \quad (5a)$$

Where,
CSCom = Cyber security compliance; measured by the banks that are in full compliance of cyber security policies and laws as given by the Central Bank of Nigeria.
ACInd = Audit committee independence; measured as the percentage of non-executive directors on the committee.
ACTech Ex = Audit committee technological expertise; measured as the number of individuals on the committee who are experienced in information technology.
ACFin Ex = Audit committee financial expertise; measured as the number of individuals on the committee who are experienced in financial knowledge
ACS = Audit committee size; measured as the amount of people on the committee as at the day of year or period end.

ε = Error term, which captures other explanatory variables that are not explicitly included in the model.
i_t = The time coefficient

4. DATA ANALYSIS AND RESULTS

This section describes the analysis of data and the use of product moment correlation and ordinary least square regression analysis to measure or test hypotheses and the objectives already stated in previous sections. The result of each of the hypothesis was also explicitly explained.

4.1. Descriptive Analysis

This presents the descriptive statistics of all the variables employed in the study of the banks as a whole.

The results obtained from the descriptive statistics shows that the average cyber security compliance for the whole sample at 1.7818%, a minimum of 1 and a maximum of 2 with a standard deviation of 0.4168%. This shows on the average that there is a high level of compliance to cyber security policies (Table 1).

The Table 2 shows the association between the dependent and independent variables of this research work. Multicollinearity between the variables is low as it shows that there is no violation of the assumption of multicollinearity since it is less than 0.7 and 0.8 which means the researcher can continue with all the independent variables.

4.2. Regression Analysis

The Table 3 clearly demonstrates the relationship and the effect of audit committee characteristics on cyber security in the Nigerian listed firms. From the Table 3, it showed that ACIND with a co-efficient of −0.0019 and a P value of 0.987 has a negative though not significant effect on cyber security. In the same vein, ACTECH EX also has insignificant negative impact with a coefficient of −0.088 and P value of 0.474 on cyber security in the banking sector. In addition, ACFIN EX has a negative coefficient of −0.103 while the P value was 0.349. However, ACSIZE was positively sign 0.084 with a P value of 0.001.

Table 1: Descriptive statistics of all the variables used in the study

Variable	Obs	Mean±SD	Min	Max
CSCom	55	1.781818±0.4168182	1	2
ACInd	55	0.6727273±0.4735424	0	1
ACTech Ex	55	0.2909091±0.4583678	0	1
ACFin Ex	55	0.6±0.4944132	0	1
ACSize	55	5.363636±2.171905	1	8

Source: Computed output (STATA, 2015)

Table 2: Test of correlation and multicollinearity between the independent variables and *CSCom*

	ACInd	*ACTech Ex*	*ACFin Ex*	*ACSize*
ACInd	1.0000			
ACTech Ex	−0.3211	1.0000		
ACFin Ex	−0.1740	0.0327	1.0000	
ACSize	−0.0982	0.1150	0.1207	1.0000

5. DISCUSSION OF RESULT AND IMPLICATION OF STUDY

The implication of the results as stated above is that, audit committee characteristics in term of ACIND, ACFIN EX, ACTECH EX have negative infl ence on the issue of cyber security in Nigeria listed banks. For example, in terms of ACIND borrowed from the assertions of PWC (2014), the report submitted that in order to maintain and improve the level of cyber security, audit committee members needed to maintain their independent perspective. Similarly, Edosa et al. (2013), stated that audit committee members that are independent of the executive directors are more likely to keep in track with their oversight functions (Walker, 2004). However, in Nigeria, the audit committee has been seen not to be fully independent of the management (Ojeka et al., 2015), hence the inability to fully provide oversight function effectively as required by the SEC Code (2011) as regard cyber security concern.

Furthermore, in term of audit committee technical expertise and cyber security, the result was also negatively signed which mean that, the level of technical expertise expected in the audit committee is lacking. Audit committee members with needed technological expertise that could ask probing questions as regard cyber security and measures that have been put in place to curb incessant attacks on the system are almost none existence (Ojeka et al., 2013). This could however mean that, before now, the issue of technological expertise among the audit committee members has not been given attention to from the management and the authority.

In addition, in term of ACFIN EX, the implication of the result showed that, the level of financial expertise among the audit committee members cannot alone enforce compliance to cyber security policies if not coupled with technical expertise. The impact was also negative to mean, there is more to what a fi ancial expert should know in order to effectively provide oversight function and monitor the development in the cyber world in order to assist the firm to reduce such attack(s). Ernst and Young (2014) stated this concerning the audit committee in Nigeria that "audit committee members are financially savvy but lack deep knowledge on technological issues".

However, the audit size was positively signed which indicate the number specified by CAMA (2004) that at least the audit committee must consist six members would be able to improve on cyber security. Majority (if not all) of the firms in Nigeria mostly comply with this provision. Anderson et al. (2004) posited that large audit committee can perform its oversight function more effectively that a smaller number by controlling and protecting the interest of the company. This means, a six member audit committee is sufficient to provide adequate oversight function and ensuring cyber security and related issues are managed effectively.

6. CONCLUSION AND RECOMMENDATIONS

The purpose of the research work was to study the impact of audit committee effectiveness on cyber security of listed Banks

Table 3: Multiple regression analysis using ordinary least square

Source	SS	Df	MS
Model	1.85575765	4	0.463939413
Residual	7.52606053	50	0.150521211
Total	9.38181818	54	0.173737374
Number of obs	55		
F (4, 50)	3.08		
P>F	0.0241		
R^2	0.1978		
Adjusted R^2	0.1336		
Root MSE	0.38797		

MSE: Mean-square error

CSCom	Coef.	Std. err.	T	P>t	95% confidence interva
ACInd	−0.0019081	0.1196485	−0.02	0.987	−0.2422292-0.2384131
ACTech Ex	−0.0881117	0.1221761	−0.72	0.474	−0.3335095-0.1572861
ACFin Ex	−0.1032651	0.1091164	−0.95	0.349	−0.3224319-0.1159016
ACSize	0.0848781	0.0246685	3.44	0.001	0.0353301-0.1344262
_cons	1.415438	0.1849944	7.65	0.000	1.043866-1.78701

Source: Computed (STATA, 2015). MSE: Mean-square error

in Nigeria by appraising the current status of the same. This paper therefore, concludes that, the presently constituted audit committee in term of its characteristics is seen not to be effective enough to provide oversight functions on cyber security in the Nigerian listed firms. Their influence is negative though not significant but for the fact that the issue of cyber security is at a front burner not just affecting firms in Nigeria, but globally. There is therefore need for the audit committee to be properly constituted and well equipped to provide oversight function over cyber issues in the sector. There is also need for training or deliberate efforts to intentionally incorporate persons with strong background in IT or in cyber issues into the committee. This can also be incorporated into the SEC governance code which is being reviewed presently so as to make it necessary for public firms to adopt

More attention should be paid to the make-up of the audit committee in term of capacity and expertise. The audit committee should be fully independent by ensuring that half of the members are independent directors as against the present non-executive directors and the remaining half which is made up of shareholders are indeed person with knowledge and expertise in information technology and cybercrime in addition to the financial expertise. The members should be sound enough to provide controls over the firm s cyber security. The reason for this is that, presently, cybercrime is the greatest threat to shareholders fund in today's world of business and especially the financial sector, there is need to protect the interest of all stakeholders, continue to create jobs opportunities, giving back to the community in term of social responsibility and of course, safeguarding the going concern of the firm

This paper has numerous advantages which can be seen from its findings. However, the study has its limitations and these are considered as opportunities for further studies. Therefore, caution should be taken when drawing conclusions from its find ngs. This paper focused on the listed bank in Nigeria and in a particular period, further studies can consider other sectors of the economy and also consider other African countries. The number of year observations could also be increased.

REFERENCES

Adeyemi, S.B., Okpala, O., Dabor, L. (2012), Factors affecting audit quality in Nigeria. International Journal of Business and Social Science, 3(20), 198-210.

Ali, A.Y., Pocock, K., Hu, Q. (2014), The effect of board of directors' IT awareness on CIO compensation and firm performance. Journal on Decision Sciences, 45(3), 401-436.

Al-Sa'eed, M., Al-Mahamid, S. (2011), Features of an effective audit committee, and its role in strengthening the financial reporting: Evidence from Amman Stock Exchange. Journal of Public Administration and Governance, 1(1), 39-62.

Anderson, R., Mansi, S., Reeb, D. (2004), Board characteristics, accounting report integrity, and the cost of debt. Journal of Accounting and Economics, 37, 315-342.

Dezoort, F., Todd, H.R., Dana, A.D., Reed, A.S. (2002), Audit committee effectiveness: A synthesis of the empirical audit committee literature. Journal of Accountancy Literature, 21, 38-75.

Ernst & Young. (2013), Viewpoints Issue 19; 2012. Available from: http://www.ey.com/publication/vwLUAssets/ACLS_viewp oints_19_May_2012/$FILE/ACLS_Viewpoints_19_May_20102.pdf.

Ernst and Young. (2014), 2014 Year-end Issues for Audit Committees. Available from: http://www.ey.com/gl/en/issues/governance-and-reporting/ey-2014-year-end-issues-for-audit-committees.

Edosa, J.A., Tina, O.A., Chijioke, O.M. (2013), Audit firm reputation and audit quality. European Journal of Business and Management, 5(7), 66-75.

Gercke, M. (2006), The slow wake of a global approach against cybercrime. Computer Law Review International, 2(2), 141.

García-Sánchez, I.M., Jose, V.F.A., Garcia-Rubio, R. (2012), Determining factors of audit committee attributes: Evidence from Spain. International Journal of Auditing, 16, 184-213.

Kalbers, L.P., Fogarty, T.J. (1993), Audit committee effectiveness-an empirical-investigation of the contribution of power. Auditing Journal of Practice and Theory, 12(1), 24-49.

Kalbers, L.P., Fogarty, T.J. (1998), Organizational and economic explanations of audit committee oversight. Journal of Managerial Issues, 10(2), 129-150.

KPMG. (2013), The Audit Committee's Oversight Role on Financial Reporting 2013. Are the Numbers too Good to Be true? Available from: https://www.assets.kpmg.com/content/dam/kpmg/pdf/2016/03/20140701_aci-oversight-2013.pdf.

Kyereboah-Coleman, A. (2007), Corporate Governance and Firm Performance in Africa: A Dynamic Panel Data Analysis. A Paper Prepared for International Conference on Corporate Governance in Emerging Markets. Available from: http://www.ifc.org/ifcext/cgf.nsf/AttachmentsByTitle/PS2.3/$FILE/KyereboahColeman+Corporate+Governance.pdf.

Lewis J.A. (2013), Raising the Bar for Cybersecurity. Washington, DC: Technology and Public Policy, Centre for Strategic and International Studies. p1-12.

Levitt, A. (2000b), Remarks before the Conference on the Rise and Effectiveness of New Corporate Governance Standards. New York: Federal Reserve Bank. Available from: http://www.sec.gov/news/speech/spch449.htm. [Last retrieved on 2011 Jun 14].

Mohuiddin, M., Karbhari, Y. (2010), Audit committee effectiveness: A critical literature review. Journal of Business and Economics, 9, 97-125.

The Nigerian Companies and Allied Matters Act (CAMA). (1990), Is Now Cited as Companies and Allied Matters Act CAP C20 LFN 2004.

Ojeka, S.A., Iyoha, F.O., Asaolu, T. (2015), Audit committee financial expertise: Antidote for financial reporting quality in Nigeria? Mediterranean Journal of Social Sciences, 6(1), 136-146.

Ojeka, S.A., Kanu, C., Owolabi, F. (2013), IFRS-based results and the readiness of Nigerian audit committee: The professional Accounting academic standpoint. European Journal of Accounting, Auditing and Finance Research, 1(4), 1-11.

Odunfa, A. (2014), Nigeria: Report on Cyber Threat Calls for Quick Passage of 2012 Bill. Available from: http://www.allafrica.com/stories/201405080279.Html.

PWC. (2014), Cyber Security: The Changing Role of Audit Committee and Internal Audit. Available from: https://www.2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf.

Raghunandan, K., Read, W., Rama, D. (2001), Audit committee composition, gray directors, and interaction with internal auditing. Accounting Horizons, 15(2), 105-118.

Rosewarne, S. (2014), Migrant domestic work: From precarious to precarisation. Journal fuer Entwicklungspolitik (Austrian Journal of Development Studies), 30(4), 133-154.

SEC Code. (2011), Corporate Governance Code. London: FRC.

Song, J., Windram, B. (2000), The Effectiveness of Audit Committee: Experience from UK, Working Paper. 12th Asian-Pacific Conference on International Accounting Issues. Beijing, China. p21-24.

United States Congress. (2002), The Sarbanes-Oxley Act of 2002, Paper Presented at 107th Congress.

Walker, R. (2004), Gaps in guidelines on audit committees. Abacus, 40(2), 157-192.

Wu, J.Y. (2012), Audit Committee Effectiveness - From the Perspective of Audit Committee Members in New Zealand Listed Companies. Lincoln.

Yermack, D. (1996), Higher valuation of companies with a small board of directors. Journal of Financial Economics, 40(2), 185-211.