Risk governance and cybercrime: the hierarchical regression approach

Erin, O, Kolawole, A & Noah, A

Original citation:
Erin, O, Kolawole, A & Noah, A 2020, 'Risk Governance and Cybercrime: The Hierarchical Regression Approach' Future Business Journal, vol. 6, 12.
https://dx.doi.org/10.1186/s43093-020-00020-1

DOI 10.1186/s43093-020-00020-1
ISSN 2314-7210

Publisher: Elsevier

Erin *et al. Futur Bus J (2020) 6:12*
https://doi.org/10.1186/s43093-020-00020-1

Future Business Journal

RESEARCH

Open Access

Risk governance and cybercrime: the hierarchical regression approach

Olayinka Adedayo Erin[1*], Adebola Daniel Kolawole[2] and Abdurafiu Olaiya Noah[3]

Abstract

This study examines the impact of risk governance on cybercrime of selected listed firms in the Nigerian financial institutions. To achieve this, a sample size of 50 listed companies from the Nigerian financial sector was selected for the years 2013–2017, resulting in 250 observations. The study employed the use of hierarchical regression analysis to test the impact of risk governance variables (Chief Risk Officer_centrality, Enterprise Risk Management_index, Chief Risk Officer_presence, Board Risk Committee_size, Board Risk Committee_activism, and Board Risk Committee_independence) and other control variables such as corporate governance variables (Board Size and Board of Directors_independence) and firm characteristics variables (Firm size and firm age) on cybercrime. The study observed from the findings that almost all the explanatory variables present a positive and significant relationship with cybercrime, except the Chief Risk Officer_presence, firm age and Board Risk Committee_size which revealed an insignificant relationship with cybercrime. The study concludes that risk governance variables and other variables are likely to reduce and minimize the impact of cybercrime on the sampled firms used in this study.

Keywords: Cybercrime, Chief Risk Officer, Enterprise Risk Management, Financial loss, Nigerian financial sector, Risk governance

Introduction

The issue of cyber risk and crime cannot be overemphasized in today's risk governance framework [1]. Recent high profile cases of cyber-attacks on financial institutions have drawn the attention of board executives, regulators, risk professionals, and academia in global discourse. Cybercrimes are becoming a global challenge facing most organizations in recent times especially, the financial organizations [2]. Regulators, board members, and stakeholders are seeking new ways to respond and detect material threats of cyber-attack on their organizations [3]. Regulators continue to issue guidelines on the risk management framework and board oversight functions on how to tackle emerging cybercrimes [4]. Evidence from the literature also shows that most financial institutions have devoted time and resources on their IT infrastructure in order to curb the menace of cybercrimes. For instance, PricewaterhouseCoopers (PwC) [5] opined that the evolving role of the board in risk governance is the major bedrock on which cybercrimes could be tackled in any organization. In support of this view, Soliman and Adam [6] posited that the governance structure of risk architecture is one of the most important factors to curb cybercrimes.

However, due to the increase in migration of financial transactions to alternative channels such mobile money, internet banking, Point-of-Sales (POS), and others, the issue of cybercrime has become a global and major challenge for financial institutions [7, 8]. This global challenge led to the International Risk Governance Council (IRGC) in 2005 developed a risk governance framework to curb the scourge of cyber threats in financial institutions. The framework viewed risk governance as a governance process effected by the entity's board to oversee risk management issues in organizations. The whole essence of risk governance is that board members are directly involved in the risk process, risk implementation, risk reporting, and disclosure [9–11].

*Correspondence: erinolayinka@yahoo.com
[1] Department of Accounting, Covenant University, Ota, Nigeria
Full list of author information is available at the end of the article

Nigeria's financial sector is of interest to this study because it has proven that the financial sector operates in a more volatile environment. Several studies argued [5, 12, 13] that firms in the Nigerian financial industry face a growing number of new and interrelated risks compared to their peers in other sectors. Nigerian financial industry risks are becoming increasingly difficult to quantify; hence, there is need to find an innovative way of reducing these risks and exposure [1]. KPMG [14] reported that financial institutions in Nigeria lose averagely about 10 billion naira yearly due to avoidable and unsystematic risk. They advocated for a more integrated and holistic approach to tackling risk issues in the Nigerian financial industry. There are fifty-seven (57) companies operating in the financial sector listed on the Nigerian Stock Exchange as at the end of 2017. Therefore, it is important for this study to focus on risk governance process as it relates to the financial sector in Nigeria.

Marjolein et al. [15] argued that due to the regulatory pressure and the effect of cyber threats, it has become necessary for the institutionalization of risk governance both in the developed and emerging countries. Several authors [10, 13, 16, 17] found that effective risk governance framework is a major step toward prevention of cybercrimes while creating sustainable future for stakeholders. These authors believed that risk governance is linked to wealth maximization of shareholders. This means the risk governance framework has the potential impact to reduce cyber-attacks that might affect the organization's bottom line.

The resultant negative effect of cybercrime on financial institutions especially in the Sub-Saharan African countries is enormous [18, 19]. Many depositors' funds and savings were lost due to the impact of cybercrimes. Estimates of about 500 million dollars in Sub-Saharan African countries are lost annually due to cyber-attacks [14]. This bad incidence has necessitated the different regulatory agencies in charge of financial institutions to strengthen the risk governance process in order to tackle fraudulent practices and cybercrimes. The purpose of risk governance is to institutionalize risk culture, strengthen risk management practices, reduce the incidence of cybercrimes, align strategic objectives with risk framework, and avoid the risk of systemic failure in financial institutions. Recent studies [4, 6, 13, 14, 20] on cybercrime in emerging economies especially African countries revealed that lack of risk oversight, poor attitude of board members, and ineffective cyber risk management have escalated the incidence of cybercrimes. The motivation for embarking on this study in Nigeria is that the issue of cybercrime has been on the increase especially in financial institutions in recent times. Therefore, it is critical to examine the impact of risk governance on cybercrime in emerging economies with a special focus on Nigeria.

Most studies on cybercrimes are from the perspectives of the audit committee, corporate governance, and e-commerce without due consideration on the subject of risk governance in Nigeria. However, few studies [6, 9, 21] on risk management framework were limited to the subject of enterprise risk management and credit risk management without holistically considering risk governance vis-à-vis its impact on cybercrimes in Nigeria. Due to the timely importance of this study on Nigerian financial institutions and other emerging economies, we are motivated to examine this study and present our findings that could help solve the menace of cybercrimes, cyber-fraud, and cyber-theft in financial institutions in Nigeria. The important question to consider is does risk governance actually impact cybercrime in financial institutions? Against this backdrop, this study seeks to examine the impact of risk governance on cybercrimes of financial institutions in Nigeria using the hierarchical regression approach. This study also recognizes other factors other than risk governance structure that could impact cybercrime.

This study proposed contribution to knowledge is in twofold. First, this study adds to the existing literature in the area of risk governance, risk management, and fraud prevention and how it affects cybersecurity issues, especially in emerging economies with Nigeria as a focus. This study provides original insight on how effective risk governance impact cybercrimes of financial institutions in emerging economies with Nigeria as a focus. Secondly, this study provides relevant information on the expanded purpose of risk governance framework within risk management research and its transformative impact on fraud and crime prevention in financial institutions.

The structure of the paper is organized as follows. "Literature review" section discusses the review of the literature on risk governance and cybercrime, also the theoretical framework that underpins the study. "Research methods" section discusses the methodology adopted as well as research design. Also, the models were specified. "Results" section presents information regarding the empirical results, and discussion was made, while "Discussion" section concludes the paper, presents recommendation and areas for further studies.

Literature review

Risk governance and cybercrime

According to the Institute of Risk Management [22], digital technologies, devices, and media have brought us great benefits as well as enormous opportunities, but their use also exposes us to significant risks. The incidences of cyber-attack have continued to be on the increase which has now made the issue of security and resilience of IT systems; their governance and management a must to improve upon by boards and top management of businesses [7]. Imperatively, it is required by those charged with risk management within a business organization to have a full understanding of the nature of its risks exposure including the available practical tools and techniques that can be deployed to mitigate those risks. Risks exposures of business cannot be divulged from various strategies evolved by senior management and the robustness of its information technology (IT), but cyber risk as asserted by IRM [22] is not purely a matter for the IT team. Cybersecurity and cyberspace are considered as the virtual world since they are abstract in nature and as such led to an increase in cybercrime activities [23]. Risk governance is the effective protective measures that can be applied in increasingly complex cybercrime landscape [24].

Risk governance advocates the use of a preventive mechanism in safeguarding vulnerable assets of an organization. Robinson [24] noted that the use of policy guided by the principle of risk management could be employed, to help prevent security breaches and minimize losses from attacks that do get through. Klinle and Renn [4] opined that risk governance combines the institutional structure and corporate policies that help organization mitigate and reduce risk problems, especially, cyber risks. IRGC [25] believed that risk governance plays a major role in the reduction in cybercrimes in today's contemporary risk environment. Therefore, it is imperative to examine the link between risk governance and cybercrime in today's financial landscape.

Risk governance determinants

Chief risk officer centrality

Liebenberg and Hoyt [26] stated that a key function of Chief Risk Officer (CRO) is to communicate risk management objectives and strategies to investors thereby ensuring greater value for firms having opaque financial health. Erin et al. [21] argued that the supervising role of a CRO ensures an effective risk governance structure. According to Erin et al. [21], all financial institutions are statutorily required to hire a CRO who will be saddled with the responsibility of overseeing risk management affairs within the organization. The study carried out by Dickinson [27] found that riskier financial institutions that have a Chief Risk Officer are more likely to form a risk management committee. Also, it is believed that the role of Chief Financial Officer (CFO) is in no way better than the CRO and that the position of CRO should not be undermined in any way [28].

Enterprise risk management

Enterprise risk management (ERM) has emerged as a construct that ostensibly overcomes limitations of silo-based traditional risk management (TRM) [9, 29]. The emergence of Enterprise Risk Management (ERM) in recent times has resulted in a new paradigm for managing the portfolio of risks that face organizations thereby making policymakers focus on mechanisms that help to improve corporate governance and risk management [27, 30]. McShane et al. [29] posited that the purpose of ERM is to gain a systematic understanding of the interdependencies and correlations among risks aggregated into portfolios, then hedging the residual risk, which is more efficient and value maximizing than dealing with each risk independently. The study used five categories of the Standard and Poor's (S&P) [31] ERM insurance rating to assess the impact of management activities on firm value for a dataset of 82 worldwide insurance companies. They found the existence of a positive relationship between an increasing level of risk management and firm value, while a change from traditional risk management to ERM does not lead to an increase in shareholder value. Risk management function and technique is largely examined using a measure called the Risk Management Index (RMI).

The study of Nocco and Stulz [32] described ERM at both macro- and micro-level stating that it enables senior management to identify, measure, and limit to acceptable levels the net exposures faced by the firm while ensuring that all material risks are "owned," and risk-return trade-offs carefully evaluated, by operating managers and employees throughout the firm. ERM gives the board and senior management the enabled capacity to effectively implement risk management framework [21]. Arumona et al. [33] in their study emphasized that the board and relevant committees should work with management to promote and actively cultivate a corporate culture and environment that understands and implements enterprise-wide risk management while recommending that risk management should be tailored to a specific company. The findings of Yong [34] showed that the successful implementation of ERM relies on corporate governance, especially periodic monitoring.

Board risk committee size

The board is charged with the overall responsibility for the oversight function of risk and risk management [33]. Going by the recent trends in corporate governance and risk management, companies have increased the proportion of independent directors and the diversity of those directors in order to enhance board performance [35]. This underscores the need to institute an independent committee within the board that will be responsible for risk management policies and framework. Financial companies covered by the Dodd-Frank Act must have dedicated risk management committees. The risk appetite and governance structure of an entity will assist in the composition of the risk committee. PwC [5] noted that risk committees provide a good way to improve board oversight of risk but not the only way to respond to the challenges.

Board risk committee activism

Board activism is the extent of involvement of a company's board of directors in the affairs of an organization while measuring the scope of a board's activities [30]. Activism promotes boardroom independence [36], and board activism increases as the proportion of outside board members increases [30]. Impliedly, it can be argued that board risk committee activism is enhanced by the proportion of independent board member in the committee. In the same vein, Boholm et al. [37] opined that board risk committee activism is intensified by the number of times the board meets in a year or quarter to discuss risk-related issues. Consistent with the view of [14, 37] revealed that board risk committee activism is indispensable in order to strengthen risk institution and governance.

Chief risk officer presence

Several studies have discussed the importance of chief risk officer [26, 35, 36] ranging from the appointment of a CRO as a part of ERM program to the influence of risk manager in driving and facilitating the ERM process in companies. Hoyt and Liebenberg [38] developed an analysis that evaluated the effects of Chief Risk Officer Presence and the board on the performance and risk of banks during the financial crisis with a specific focus on the European banks. Findings from the study showed that the sole presence of the CRO is not sufficient to reduce the riskiness of the bank but seems to increase risk. Although findings from the study of [13, 30] did not indicate any financial benefit for the shareholders in those companies that hired CRO.

Board risk committee independence

The independence of the risk committee is pivotal to risk management activities of any organization [39]. It is expected that the risk governance process is founded on sound corporate governance principles. Studies of [12, 13] argued that the inclusion of independent persons in the risk committee will further strengthen the risk culture, risk architecture, and risk disclosure. Also, the study of Peters et al. [40] revealed that independent directors that are knowledgeable in risk and financial matters are skilled in financial models in evaluating projects that have a positive and significant impact on the organization.

Other factors

Corporate governance determinants

Board of directors independence Board independence is a central issue in risk governance practice. Board independence is to ensure that the board is objective enough to act in the best interests of the company's stakeholders [41]. It is the responsibility of the board to provide oversight function regarding risk strategy, risk implementation, risk compliance, and risk disclosure [30]. However, the board of directors in many organizations are unaware of their responsibility in developing and providing management guidance regarding risk management strategy within the organization. Decker and Galer [42] revealed that the board of director independence is a crucial factor in risk governance in any organization. The independence of the board should be clearly distinct from the management's responsibility of implementing the risk strategies developed by the board of directors. The study of Beasley et al. [30] found that the board of director independence positively influenced ERM implementation among firms.

Board size The size of the board is one of the major determining factors in corporate governance principle [43]. Similarly, Rochette [44] argued that firms with high board size have a greater tendency to adopt a holistic risk management system and follow the risk governance process. Also, Pagach and Warr [13] revealed that board size plays a determining factor in risk governance, risk implementation, and risk disclosure. Consistent with the view of Rochette [44] and Beasley et al. [30] found that most financial institutions with diverse board members are likely to adopt a holistic approach in tackling the issue of cybercrimes and ensure strict risk governance process.

Firm characteristics determinants

Firm age The subject of firm age appeared in most empirical research in finance. It is mostly used as a control variable in studies on firm performance [45], corporate diversification [46], ownership structure [47], and risk management research [13]. Firm age is viewed as the number of years of incorporation [48], even though some authors argued that firm age starts when it is listed [29]. The subject of firm age is contentious in research; however, studies opined that the age of a firm is a key determinant in firm's sustainability, performance, and survival [49–51].

Firm size It is believed that when organization size increases, it is bound to experience different threatening events (risk) that could affect the business sustainability.

Beasley et al. [30] found that larger firms are more likely to commit greater resources to their risk management activities. The study of Ilaboya and Ohiokha [48] found that larger firms are more likely to take the issue of risk governance more serious than smaller firms. In tandem with this view, [7] revealed that larger firms have higher risk exposure and greater financial distress and as a result, they are more likely to implement integrated risk management and put more attention on risk governance process. Previous studies [30, 52] found a positive correlation between firm size and risk management activities. It thus means that larger firms are more willing to allocate more resources to tackle the issue of risks affecting their business operations.

Based on the above issues, the study hypothesized is developed:

H_0 Risk governance has no significant impact on cybercrime of firms operating in the Nigerian financial sector.

Conceptual model

The conceptual model depicts the various variables or factors that affect cybercrime (Fig. 1).

The conceptual framework forms the basis on which this study is anchored and is linked to the research hypothesis.

Literature gaps

Previous research has been limited in empirically showing the relevance of risk management in financial institutions in Nigeria [6, 9, 49, 53–55]. The research gap identified with these previous studies only examined risk management from the perspective of firm performance and firm value without holistically considering the impact of risk governance on cybercrime. Also, previous studies have only been limited to the banking sector without researching the financial sector as a whole. Against this backdrop, this study seeks to extend the frontier of knowledge by filling the identified gap.

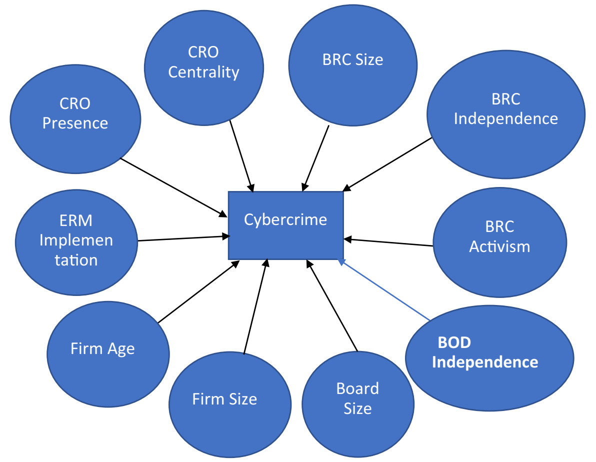

Fig. 1 Conceptual model. *Source*: Developed by Authors

Theoretical consideration

The theory of legitimacy has been a popular theory in the field of management and accounting in recent times. It is important due to its ability in analyzing the relationship between companies and their environment. Dowling and Pfeffer [56] opined that legitimation is a process where the organization has the right to transform, import, and export information within the organizational context. Legitimacy theory is derived organizational legitimacy which means a firm's value system is congruent within the large social system of which the firm is a part. Deegan [57] considered the legitimacy theory as a social contract between the organization and the society in which it operates. They argued that values and norms within the society are not fixed but continuously changing over time. The continuous societal value has heightened social expectation; therefore, for the organization to be successful, it has to be attentive to societal (environmental, human, and social) needs. Risk management and governance are considered as a legitimate function the organization has to fulfill in order to create value for its stakeholders [58, 59]. Many researchers argued that risk management and governance must meet the societal needs in order to be considered relevant and successful especially in mitigating cybercrimes [30, 60, 61].

Most studies viewed legitimacy theory with respect to organizational dynamics and value creation in determining risk governance process [6, 62]. These authors argued that societal pressure was heightened after the corporate scandals experienced in recent times. These corporate failures increased regulatory and stakeholders' pressure on the need for organizations to adopt more rigorous corporate governance and risk management framework in creating value and performance. Some studies revealed that is legitimate for the organization to adopt a risk process that will facilitate the firm's performance, growth and reduce cybercrimes. Mikes and Kaplan [63] considered legitimacy has an important resource in which organization is dependent for its survival. Their study claimed that legitimacy as a resource can be achieved through disclosure strategies. Also, Bromiley et al. [12] and Shima et al. [64] explained that in recent times, corporate legitimation strategies have increased focus on risk management practices with regard to firm's reputation. Reputation risk studies emphasized the importance of legitimacy theory for financial growth of the organization. It is considered a good resource for future profit which invariably affects the firm's long-term sustainability.

Research methods

Research design

This study employed panel data to examine the impact of risk governance on cybercrime of listed firms operating in financial institutions in Nigeria. This study covers the period of 2013–2017. Data were gathered across the firms over a period of five (5) years (2013–2017). The reason for the choice of the period was that the regulatory authority (Central Bank of Nigeria) in Nigeria to develop holistic risk governance framework in the Nigerian financial institutions in the year 2012 to tackle the problem of cybercrime. The CBN risk governance framework placed more emphasis on the function of the risk management committee, risk governance process, the role of the board of directors as well as developing a holistic risk management framework. Therefore, it is important to critically investigate the impact of risk governance system on cybercrimes in the Nigerian financial institutions for the period of 2013–2017.

The study population consists of fifty-seven (57) firms listed on the Nigerian Stock Exchange (NSE) for the specified period. Based on Taro Yamane sampling formula, the sample size was limited to fifty (50) firms (see "Appendix 1" section). We gathered our data from the annual reports of selected firms and from African financial report. This study focused on financial institutions because of its stabilizing role in the economy and its ability to prevent a systemic collapse of the entire economic system. The data were analyzed through descriptive statistics, Pearson correlation, and hierarchical regression method.

Measurement of variables

In this section, we examined the variables used in this study ranging from the dependent variable to independent variables; however, the same set of variables were used in all the study periods, respectively (Table 1).

> *ERM_Index* This is derived from both corporate governance measure and risk assessment procedure. The first three variables from corporate governance (CG) measure are:
> Presence of CRO-1

Table 1 Measurement and operationalization of variables. *Source*: Developed by Authors

Variable(s)	Symbols	Operationalization	Prior studies
Dependent variable			
Financial loss (cybercrime)	*FINLoss*	Proxy by the total financial loss suffered due to cybercrime disclosed in the annual reports	Baxter et al. [23] and Okoye et al. [65]
Independent variables (risk gov. variables)			
Chief risk officer presence	*CRO_presence*	CRO is dummy variable, set equal to 1 for firms with CRO designation, and 0 otherwise	McShane et al. [29]
Chief risk officer centrality	*CRO_centrality*	CRO remuneration divided by CFO remuneration. Note CFO means Chief Financial Officer	Cavezzali, and Garddenal [66]
Board risk committee size	*BRC_size*	The total number of members on the risk committee	Erin et al. [21] and [33]
Board risk committee activism	*BRC_activism*	BRC activism is the number of times meeting was held in a financial year	Aebi et al. [67] and Li et al. [20]
Enterprise risk management index	*ERM_index*	ERM index is measured through the combination of corporate governance and risk variables	Hoyt and Liebenberg [38] and Arnold et al. [68]
Board risk committee independence	*BRC_independence*	The proportion of non-executive directors divided by total numbers of directors	Gordon et al. [16] and Soliman and Adam [6]
Corporate governance variables			
Board of director independence	*BOD_independence*	The proportion of non-executive directors divided by total numbers of directors	Ellul and Yerramilli [41];
Board size	*BSIZE*	The actual number of directors on the firm's board	Ame, Arumona and Erin [45]
Firm characteristics variables			
Firm Age	*FAGE*	The number of years of a firm's existence since incorporation	Baxter et al. [23] and Okoye et al. [43]
Firm size	*FSIZE*	Proxy by the natural logarithm of Total Assets	Uwuigbe et al. [47]

Risk Committee-2
Reporting frequency between Risk Committee (RC) and board of directors (BOD)—3
The other three variables from risk assessment procedure measure are:
Risk Assessment frequency (RA_frequency)-4
Risk Assessment Level (RA_level)-5
Risk Assessment Methodology (RA_Method)-6
The comprehensive ERM_Index is the sum of all the six variables that ranges from 1 to 6. ERM_Index rates firms from numbers 1 to 6 depending on the level of their ERM implementation.

Model specification

We developed our models based on the conceptual issues reviewed in the literature. This model captured the risk governance variables (main predictor variables) examined in the literature in this study. The estimated econometric model is expressed in the following equations:

Model 1

$$\begin{aligned} FINLoss = f\ \big(&CRO\_centrality,\ ERM\_index, \\ &BRC\_size,\ BRC\_activism, \\ &CRO\_presence,\ BRC\_independence) \end{aligned} \quad (1)$$

$$\begin{aligned} FINLoss_{it} = \beta_0 &+ \beta_1 CRO\_centrality_{it} \\ &+ \beta_2 ERM\_index_{it} + \beta_3 BRC\_size_{it} \\ &+ \beta_4 BRC\_activism_{it} \\ &+ \beta_5 CRO\_presence_{it} \\ &+ \beta_6 BRC\_independence_{it} \mu_{it} \end{aligned} \quad (2)$$

where FINLoss = Financial Loss, *CRO_centrality* = Chief Risk Officer Centrality, *ERM_index* = Enterprise Risk Management Index, *BRC_size* = Board Risk Committee Size, *BRC_activism* = Board Risk Committee Activism, *CRO_presence* = Chief Risk Officer Presence, *BRC_independence* = Board Risk Committee independence, $i = 1$, 2, 3, ..., 50 indicating the number of firms that were used for the study, $t = 1, 2, \ldots, 5$ indicating the time period that was used for this study (2013–2017), $\beta 1{-}6$ = coefficient or slope of the regression line or independent variables. μ_{it} = The error term which accounts for other possible factors that could affect the dependent variable not captured in the model (the stochastic error term is assumed to be identically and independently distributed).

Model 2

In order to use the hierarchical regression method, there are other corporate governance variables (other than the main predictor variables) that were added to know if it has more impact on the dependent variable. The econometric model is stated below:

$$\begin{aligned} FINLoss_{it} = \beta_0 &+ \beta_1 CRO\_centrality_{it} \\ &+ \beta_2 ERM\_index_{it} + \beta_3 BRC\_size_{it} \\ &+ \beta_4 BRC\_activism_{it} + \beta_5 CRO\_presence_{it} \\ &+ \beta_6 BRC\_independence_{it} \\ &+ \beta_7 BOD\_independence_{it} \\ &+ \beta_8 BSIZE_{it} + \mu_{it} \end{aligned} \quad (3)$$

where *BOD_independence* = Board of Directors Independence, BSIZE = Board Size, $i = 1$, 2, 3, ..., 50 indicating the number of firms that were used for the study, $t = 1, 2, \ldots, 5$ indicating the time period that was used for this study (2013–2017), $\beta 1{-}8$ = Coefficient or slope of the regression line or independent variables. μ_{it} = The error term which accounts for other possible factors that could affect the dependent variable not captured in the model (the stochastic error term is assumed to be identically and independently distributed).

Model 3

In order to further test the impact of risk governance on cybercrime, there are two firm characteristics variables that were added. The econometric model is stated below:

$$\begin{aligned} FINLoss =_{it}= \beta_0 &+\ \beta_1 CRO\_centrality_{it} \\ &+\ \beta_2 ERM\_index_{it} +\ \beta_3 BRC\_size_{it} \\ &+\ \beta_4 BRC\_activism_{it} +\ \beta_5 CRO\_presence_{it} \\ &+\ \beta_6 BRC\_independence_{it} \\ &+\ \beta_7 BOD\_independence_{it+} \beta_8 BSIZE_{it} \\ &+ \beta_9 FAGE_{it} +\ \beta_{10} FSIZE_{it} + \mu_{it} \end{aligned} \quad (4)$$

where FAGE = Firm Age, FSIZE = Firm Size, $_{\mathrm{i}} = 1$, 2, 3, ..., 50 indicating the number of firms that were used for the study, $t = 1, 2, \ldots, 5$ indicating the time period that was used for this study (2013–2017), $\beta 1{-}10$ = Coefficient or slope of the regression line or independent variables. μ_{it} = The error term which accounts for other possible factors that could affect the dependent variable not captured in the model (the stochastic error term is assumed to be identically and independently distributed).

Data analysis techniques

This study employed the hierarchical regression method to measure the impact of risk governance on cybercrime. The essence of hierarchical regression is to show if variables examined explain statistically significant variance in the dependent variable. Since hierarchical regression is a model comparison analysis, therefore, there is a need to account for other variables other than the main predictor variables. The study also conducted preliminary statistical analysis like descriptive statistics and correlation matrix, measurement of variables' normality, and their relationship, respectively.

Table 2 Descriptive statistics

	FinLoss	CRO_centrality	ERM_index	BRC_size	BRC_activism	CRO_presence	BRC_indp	BOD_indp	BSIZE	FAGE	FSIZE
Mean	23.9681	0.3126	4.3400	3.8245	3.8729	0.8100	2.1220	3.4199	8.8560	38.4600	124.3737
Median	22.7770	0.2845	4.0000	3.2347	3.4596	0.7800	2.0000	3.1223	7.5954	31.0000	114.9870
Maximum	42.7625	0.5375	6.0000	5.0000	6.0000	1.0000	3.0000	4.0000	10.0000	73.0000	252.3875
Minimum	2.2780	0.1157	3.0000	3.0000	2.0000	0.0000	1.0000	2.0000	6.0000	17.0000	39.9011
SD	10.8646	0.8829	0.8829	0.1071	0.8653	0.4499	0.1120	0.1050	2.3257	23.5973	5.7355
Skewness	1.3306	0.9783	0.1589	0.1685	1.4253	-0.9854	0.5022	0.1463	1.1901	1.3471	0.7499
Kurtosis	2.5150	2.7663	2.3095	1.6551	2.1168	1.9603	2.1929	2.6278	2.6886	2.1013	1.9961
Jarque–Bera	76.5431	45.3903	6.0188	20.0239	97.6401	51.2732	17.2959	2.3357	63.9628	121.6178	33.9307
Probability	0.0000	0.0687	0.0493	0.0000	0.0045	0.0000	0.0001	0.3110	0.0000	0.0000	0.3217
Sum	274.2035	17.8637	108.5000	56.1250	93.2401	18.0000	30.5000	104.9931	22.1400	96.1500	25.9343
Sum Sq. Dev.	23.9212	19.4100	15.5328	2.8593	34.7433	50.4000	3.1290	2.7473	13.4681	13.6521	81.9359
Observations	250	250	250	250	250	250	250	250	250	250	250

Results

Univariate analysis

Table 2 presents the descriptive statistics for all variables. Looking at the risk governance variables, the result of CRO_presence revealed that 81% of firms operating in financial institutions have a designated CRO to oversee the risk management department and other risk-related activities. The mean value of ERM_index showed 4.34, which means that 72% (4.34/6) firms have an ERM framework in place to manage risk activities. This result signifies a commitment to holistic risk management practices and the adoption of a more integrated risk system to tackle emerging risks. The BRC_size showed a maximum value of 5, the minimum value of 3, and a mean value of 3.8. This suggests that approximately, there are 4 members that constitute the risk committee. This is in line with the Central Bank of Nigeria (CBN) guidelines that members of the risk committee must not be less than 3. Considering the BRC_independence, the result showed that at least 2 members are independent members; it means that 50% of the risk committee are independent members. The result of CRO_centrality shows 31%, and this signifies that 69% (1–31) of CFO earns a higher salary or remuneration than CRO of firms operating in the Nigerian financial sector. The result of the BRC_activism shows that on the average board members meet 3 or 4 times a year to discuss issues relating to risk activities.

Also, the table shows the results of corporate governance and firm characteristics variables, and the result of the board size (BSIZE) revealed that the maximum number of directors stand at 10, while the minimum number is 6. The mean value showed 8.85; this implies that on the average the composition of the board ranges from 8 to 9 members. The BOD_independence showed that at least 3 non-executive directors are represented on the board. It means that (3.41/8.85) 39% of the board are represented by independent directors, and this is above the regulatory benchmark of 25% stipulated by the Securities and Exchange Commission [69]. The average age of firms is 38 years, while the lowest is 17 years; this implies that firms in this sector are relatively old.

Bivariate analysis

Table 3 shows the correlation coefficients of the variables examined to measure cybercrimes (financial loss) used in the study. As observed, CRO_centrality is positively related to financial loss. The same is observed for ERM_index, BRC_size, BRC_activism, BOD_independence, BSIZE, FAGE, and FSIZE, while CRO_presence and BRC_independence revealed a negative relationship with cybercrime (financial loss). This result suggests that risk governance is more likely to have a significant impact on cybercrime of firms operating in the Nigerian financial institutions. The positive relationship between ERM_index and financial loss proves that the firms with the ERM framework are more likely to reduce the impact of cybercrime. Also, the relationship between FSIZE and financial loss suggests that larger firms are more likely to deploy sophisticated risk infrastructure to tackle emerging risks and issue of cybercrimes. However, CRO_presence showed a negative relationship with financial loss; this means that the presence of CRO alone might not be able to tackle cybercrime. The significance of this relationship shows that the size of board risk committee and the number of times board risk committee meets are important in the risk governance process.

In order to confirm the existence of collinearity among the variables, we tested the variance inflation factor as shown in Table 4. The centered variance inflation factor showed that the variables are clustered around the value of 5.00; this signifies the absence of multicollinearity. The assumption is that if the centered variance inflation factor is beyond the value of 10; there is an indication of multicollinearity [70].

Multivariate analysis

The result of the hierarchical regression analysis is presented in Table 5. Model 1 presents the risk governance variables that are linked with the dependent variable (financial loss). The result showed a positive and significant relationship between the CRO_centrality $(0.0192 < 0.05)$ and financial loss. Also, ERM_index $(0.0219 < 0.05)$, BRC_activism $(0.0001 < 0.05)$, and BRC_independence $(0.0178 < 0.05)$ reported a positive and significant relationship with financial loss. On the contrary, CRO_presence $(0.7438 > 0.05)$ showed a negative and insignificant relationship with financial loss. The same with BRC_size $(0.7686 > 0.05)$ which presented an insignificant relationship with financial loss. The Durbin–Watson statistic of 2.01613 is not substantially different from the 2.00 benchmark which indicates the absence of serial correlation. The adjusted R^2 value of model 1 revealed 51% shows an average explanatory power of the independent variables.

Considering the model 2 where corporate governance variables (BSIZE and BOD_independence) were added to risk governance variables to test its impact on cybercrimes. From the above analysis, BOD_independence $(0.0339 < 0.05)$ and BSIZE $(0.0473 < 0.05)$ showed a positive and significant relationship with financial loss. This confirmed the increase in adjusted R^2 from 51 to 55%, which represented a 7% increase. This result implies that the addition of the two corporate governance variables (BSIZE and BOD_independence) have a slight impact

Table 3 Summary of correlation coefficients

	FinLoss	CRO_centrality	ERM_index	BRC_size	BRC_activism	CRO_presence	BRC_indp	BOD_indp	BSIZE	FAGE	FSIZE
Covariance analysis: ordinary											
Included observations: 250											
FinLoss	1										
CRO_centrality	0.0605	1									
ERM_index	0.2701	0.1325	1								
BRC_size	0.2184	0.1383	0.6392	1							
BRC_activism	0.3024	0.0967	0.8735	0.5657	1						
CRO_presence	−0.2181	0.0337	0.1778	0.2085	0.0924	1					
BRC_indp	−0.0794	0.0441	−0.2012	−0.1931	−0.3143	−0.0061	1				
BOD_indp	0.1983	0.1683	0.8887	0.6149	0.8297	0.1654	−0.2445	1			
BSIZE	0.0577	0.1015	0.4677	0.4449	0.4964	0.0976	0.0297	0.4845	1		
FAGE	0.2649	0.1579	0.9858	0.6431	0.8748	0.1924	−0.2317	0.3412	0.4539	1	
FSIZE	0.1983	0.1683	0.8887	0.6149	0.8297	0.1454	−0.2492	−0.2753	0.8983	0.4512	1

Table 4 Variance inflation factor

Variable	Coefficient Variance	Uncentered VIF	Centered VIF
CRO_centrality	0.265824	387.0853	5.016739
ERM_index	0.129085	109.4423	4.094435
BRC_size	0.116149	136.7418	3.430158
BRC_activism	0.410843	469.9366	5.513016
CRO_presence	0.120812	197.1440	2.153256
BRC_indp	0.092319	208.0975	3.552856
BOD_indp	0.179142	333.7813	3.184675
BSIZE	0.120914	352.2471	3.452202
FAGE	0.031248	229.2859	4.452202
FSIZE	0.196831	371.7835	4.957021

on cybercrime of selected firms in this study. In model 3, firm attributes variables (FSIZE and FAGE) were added to the existing models to determine its impact on cybercrime. Following the above analysis, only FSIZE ($0.0469 < 0.05$) showed a positive and significant relationship with the financial loss, while FAGE showed otherwise. However, there is an increased adjusted R^2 from 55 to 57%, representing only 4% improvement. In the overall, the addition of corporate governance and firm characteristics variables increase the adjusted R^2 from 51 to 57% which gives 11% increase. Also, the Durbin–Watson statistic for models 2 and 3 showed 2.15391 and 1.92172, respectively. It is not substantially different from the 2.00 benchmark which indicates the absence of serial correlation among the variables.

Discussion

Restatement of hypotheses and discussion of findings

H_0 Risk governance has no significant impact on cybercrime of firms operating in the Nigerian financial sector.

The hierarchical regression analysis focused on the impact of risk governance on cybercrime while the analysis controlled for other variables. From the regression result, the CRO_centrality value ($p = 0.019 < 0.05$) showed a positive and significant relationship with cybercrime. The same is observed for ERM_index ($p = 0.021 < 0.05$), BRC_activism ($p = 0.001 < 0.05$), BRC_independence ($p = 0.017 < 0.05$), BOD_independence ($p = 0.033 < 0.05$), BSIZE ($p = 0.047 < 0.05$), FSIZE ($p = 0.047 < 0.05$) which revealed a positive and significant relationship with cybercrime. On the other hand variables such as CRO_presence ($p = 0.743 > 0.05$), BRC_size ($p = 0.768 > 0.05$), and FAGE ($p = 0.147 > 0.05$) showed an insignificant relationship with cybercrime. In overall, the regression result showed that there is a significant relationship between risk governance and cybercrime of selected firms operating in the Nigerian financial sector. Therefore, the null hypothesis is rejected.

The foregoing results present a major implication on the subject of risk governance vis-à-vis its impact on cybercrimes. The positive relationship between ERM_index and cybercrime suggests that effective implementation of ERM framework has the capacity to reduce the threats of cybercrimes. This finding is consistent with the studies of [28, 38]. These studies documented that the risk governance process improves firm value, firm performance, and reduces the threats of emerging risks. This is

Table 5 Hierarchical regression analysis

Variable	Model 1			Model 2			Model 3		
	B	SE B	*β*	B	SE B	*β*	B	SE B	*β*
CRO_centrality	0.357729	2.653295	0.0192*	0.480595	0.178433	0.0209*	− 1.145268	0.651863	0.0797
ERM_index	0.295916	2.185682	0.0219*	0.122088	0.39216	0.0458*	0.455905	0.031593	0.0576*
BRC_size	0.328536	1.115555	0.7686	0.052798	0.044063	0.2318	− 0.009177	0.002983	0.0722
BRC_activism	0.63852	0.102648	0.0001*	0.010103	0.005212	0.0536*	0.004284	0.011645	0.0221*
CRO_presence	− 0.022859	0.069892	0.7438	0.13199	0.015101	0.0153	0.280285	0.012879	0.2412
BRC_indp	0.148971	0.06256	0.0178*	0.494993	0.018938	0.0007*	− 0.013179	0.042683	0.0077*
BOD_indp				0.366874	0.078328	0.0339*	0.005837	0.001452	0.0001*
BSIZE				− 0.00096	0.00138	0.0473*	0.019721	0.012212	0.0072*
FAGE							0.315561	0.290121	0.1474
FSIZE							0.420458	1.250831	0.0469*
R^2		0.52			0.57			0.59	
Adjusted R^2		0.51			0.55			0.57	
Adjusted R^2 change		0.00			0.04			0.02	
Durbin–Watson stat		2.01613			2.15391			1.92172	

*5% level of significance

a clarion call to institutionalize effective risk governance process in order to curb the menace of cybercrime and attacks. The assumption is that a sound risk management framework is likely to minimize emerging risks, especially for firms in financial institutions. Also, the BRC_independence revealed a positive and significant relationship with cybercrime. This implies that independent directors are important in risk governance and strategy. Therefore, there is need to hold senior management accountable for the overall risk management and execution. This result is in tandem with the studies of [6, 13, 21].

Furthermore, the regression result revealed a positive and significant relationship between BRC_activism and cybercrime. From the findings, risk committee members meet about 4 times in a year to discuss risk-related matters. This underscores the importance of risk issues in financial institutions in Nigeria; this suggests that members of the risk committee are more committed and concerned about risk issues affecting the organization. This corroborates the findings of [29, 39] which document a positive relationship between BRC_activism and firm performance. The findings on CRO_centrality prove that CRO officers are critical to risk governance in any organization. Even though the results showed that CFO collects high remuneration than CRO for the firms used in this study. This does not undermine the role of CRO executing risk governance functions and other oversight duties.

Furthermore, the results showed other factors that affect cybercrime other than risk governance variables. Variables such as BOD_independence, BSIZE, and FSIZE revealed a positive and significant relationship with cybercrime. This implies it takes holistic efforts to tackle the problem of cybercrime in any organization. Most studies argued that the size of the firm contributes to its performance and sustainability. Larger firms are expected to face more complex risks than smaller firms; therefore, the large firms are more likely to take a sophisticated and integrated approach in tacking the issue of cybercrimes. This is in agreement with the study of [9, 71] which found that larger firms are more likely to have a sound and robust risk governance system. The inclusion of independent directors with risk management expertise on the board has the possibility of influencing decisions relating to risk management in the organization.

On the contrary, CRO_presence and firm age revealed a negative and insignificant relationship with cybercrime. This result suggests that the presence of CRO alone is not sufficient to tackle wide and emerging risks confronting organization today. Quite a number of studies found that hiring of CRO does not necessarily reduce the impact of risk on the organization [6, 13, 26, 36]. Consistent with this view, Ernst and Young [2] opined that the position of CRO is indispensable but cannot alone carry out his mandate without the support of senior management and all business units. The insignificant relationship between firm age and cybercrime implies that the age of a firm does not matter on the issue of cybercrime or attack. What matters to perpetrators of crime is the target they are aiming at; not the age of a firm.

The practical implications of this study provide valuable information for board of directors and those saddled with risk governance process. The direct participation of the board in risk governance issues affect to a large extent in curbing the issues of cybercrime. Also, this study helps inform regulatory agencies and policy makers on the need for firms to provide comprehensive and qualitative risk information to their stakeholders. In the same vein, this study provides insight for listed firms in the financial sector in Nigeria on how to satisfy the continuous yearning for the voluntary reporting of qualitative risk disclosure and information.

This finding also corroborates the legitimacy theory which asserts that firms should adopt a risk governance process that will facilitate the firm's performance, growth, and reduce cybercrimes.

Conclusion, limitation, and contribution

This study focused on examining whether risk governance impact cybercrime of firms operating in financial institutions in Nigeria. The approach followed was to analyze fifty (50) selected firms for the period of 2013–2017 using the hierarchical regression analysis. The study observed from the findings that almost all the explanatory variables present a positive and significant relationship with cybercrime, except the CRO_presence, firm age, and BRC_size which revealed an insignificant relationship with cybercrime. The study used the risk governance variables (CRO_centrality, ERM_index, CRO_presence, BRC_activism, BRC_size, and BRC_independence); corporate governance variables (BOD_independenc, BSIZE) and firm characteristics variables (FSIZE, FAGE) as independent variables to determine their impact on cybercrime. The study concludes that risk governance variables and other variables are likely to reduce and minimize the impact of cybercrime of the sampled firms used in this study.

This study contributes to the growing research in the area of risk management, risk governance, cybersecurity in emerging economies especially the Sub-Saharan countries. The empirical approach used in investigating the effect of risk governance on cybercrime contributes to the quality of this research in the area of risk management research which reinforces the originality of this study. To the best of the authors' knowledge, this is the first study that used the combination of these variables to measure the impact of risk governance on cybercrime in emerging economies. We suggest that financial institutions should be more integrated, strategic, forward-looking, effective, and practical in their approach to tackling the issue of cybercrimes and attacks. Also, we believe that stronger board oversight, robust risk culture, increased risk accountability, and improved risk transparency will go a long way to minimize the threat of cybercrime in today's financial landscape. This research was limited to firms of financial institutions in Nigeria; however, the study sets the tone for future empirical research on the subject matter. This study provides an avenue for future research in the area of risk governance and cybercrime in Africa. Further studies could also research into the comparative analysis of African countries compared to other continents of the world in the area of risk governance and cybercrime. Also, future studies could incorporate other firm-level controls such as return on assets, return on equity, and liquidity ratios.

Abbreviations

CRO: Chief Risk Officer; CFO: Chief Financial Officer; CBN: Central Bank of Nigeria; BRC: Board Risk Committee; ERM: Enterprise Risk Management; IRGC: International Risk Governance Council; IRM: Institute of Risk Management; RMI: Risk Management Index; TRM: Traditional risk management; POS: Point of sale.

Authors' contributions

ADK contributed by writing the literature review of this paper. OAE analyzed and interpreted the data set for this study. OAE also worked on the methodology section. AON contributed by writing the introductory section of the paper and performed general editing of the manuscript. All authors read and approved the final manuscript.

Funding

There is/are no funding available for this research from any institution.

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Consent for publication

The authors give their consent for this article to be published.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] Department of Accounting, Covenant University, Ota, Nigeria. [2] Afe Babalola University, Ado-Ekiti, Nigeria. [3] Coventry University, Coventry, UK.

Appendix 1

S/N	Companies	Industry
1	Access Bank	Banks
2	Diamond Bank	Banks
3	UBA	Banks
4	First Bank Plc	Banks
5	FCMB Plc	Banks
6	Fidelity Bank	Banks
7	GTBank	Banks
8	StanbicIBTC	Banks
9	SterlingBank	Banks
10	Ecobank	Banks
11	UnityBank	Banks
12	Wema Bank	Banks
13	UnionBank	Banks
14	Skyebank	Banks
15	Zenith Bank	Banks
16	AIICO	Insurance
17	African Alliance Insurance	Insurance
18	Cornerstone Insurance	Insurance
19	Consolidated Hallmark	Insurance
20	Intl Energy Insurance	Insurance
21	Law Union and Rock Insurance	Insurance
22	Niger Insurance	Insurance
23	Mutual Benefit Insurance	Insurance
24	Standard Alliance Insurance	Insurance
25	Unity Kapital Insurance	Insurance
26	UNIC Insurance	Insurance
27	Prestige Assurance Co. Plc	Insurance
28	Linkage Assurance	Insurance
29	Custodian and Allied Insurance Plc	Insurance
30	Mansard Insurance Plc	Insurance
31	Continental Reinsurance Plc	Insurance
32	Guinea Insurance Plc	Insurance
33	Equity Assurance Plc.	Insurance
34	Goldlink Insurance Plc	Insurance
35	Great Nigerian Insurance Plc	Insurance
36	NEM Insurance Plc	Insurance
37	Investment And Allied Assurance	Insurance
38	Lasaco Assurance Plc.	Insurance
39	Regency Alliance Insurance	Insurance
40	Sovereign Trust Insurance Plc	Insurance
41	Wapic Insurance Plc	Insurance
42	Universal Insurance Company	Insurance
43	Royal Exchange Plc	Insurance
44	United Capital Plc	Investment
45	Union Homes Savings And Loans Plc.	Investment
46	Deap Capital Mgt. and Trust Plc	Investment
47	Africa Prudential Registrars Plc	Investment
48	Abbey Mortgage Bank Plc	Investment
49	Nigeria Energy Sector Fund	Investment
50	Aso Savings and Loan	Investment

Received: 9 July 2019 Accepted: 26 February 2020
Published online: 28 May 2020

References

1. Kaplan J, Bailey T, O'Halloran D, Marcus A, Rezek C (2015) Beyond cybersecurity: protecting your digital business. Wiley, Berlin. https://doi.org/10.1002/9781119055228
2. Ernst & Young (2017) The evolving role of the board in cyber security risk oversight. https://www.eycom.ch/en/Publications/20170901
3. Zemzem A, Kacem O (2014) Risk management, board characteristics and performance in the Tunisian lending institutions. Int J Finance Bus Stud 3(1):186–200
4. Klinle A, Renn O (2011) Adaptive and integrative governance on risk and uncertainty. J Risk Res 15(3):273–292. https://doi.org/10.1080/13669877.2011.636838
5. PriceWaterhouseCoopers (PWC) (2017) Enterprise risk management: an Integrated framework. Committee of Sponsoring Organisations of the Tread way Commission. https://www.pwc.com/us/en/cfodirect/standard-setters/coso.html
6. Soliman A, Adam M (2017) Enterprise risk management and firm performance: an integrated model for the banking sector. Banks Banks Rev 12(2):116–123. https://doi.org/10.21511/bbs.12(2).2017.12
7. Fadun O (2013) Risk management and risk management failure: lessons for business enterprise. Int J Acad Res Bus Soc Sci 3(2):225–241
8. Steinbart P, Raschke R, Gal G, Dilla W (2012) The relationship between internal audit and information security: an exploratory investigation. Int J Account Inf Syst 13(3):228–243. https://doi.org/10.1016/j.accinf.2012.06.007
9. Erin O, Eriki E, Arumona J, Ame J (2017) Enterprise risk management and financial performance: evidence from an emerging market. Int J Manag Account Econ 4(9):937–952
10. Kakanda M, Salim B, Chandren S (2017) Corporate governance, risk management disclosure, and firm performance: a theoretical and empirical review perspective. Asian Econ Financ Rev 7(9):836–845
11. Liaropoulous A, Sapountzaki K, Nivolianitou Z (2016) Risk governance gap analysis in search and rescue at offshore platforms in the Greek territory. Saf Sci 86:132–141. https://doi.org/10.1016/j.ssci.2016.02.013
12. Bromiley P, McShane M, Nair A, Rustambekov E (2014) Enterprise risk management: review, critique, and research directions. Long Range Plan 2(1):1–12. https://doi.org/10.1016/j.lrp.2014.07.005
13. Pagach D, Warr R (2011) The characteristics of firms that hire chief risk officers. J Risk Insur 78(1):185–211. https://doi.org/10.2139/ssrn.1010200
14. KPMG (2016) Risk governance: a benchmark analysis of systemically important banks. http://www.kpmg.com. Accessed 07 Jan 2019
15. Marjolein B, Van A, Renn O (2011) Risk governance. J Risk Res 14(4):431–444. https://doi.org/10.1080/13669877.2011.553730
16. Gordon L, Loeb M, Tseng C (2009) Enterprise risk management and firm performance: a contingency perspective. J Account Public Policy 28(4):301–327. https://doi.org/10.1016/j.jaccpubpol.2009.06.006
17. Quon T, Zeghal D, Maingot M (2012) Enterprise risk management and firm performance. Proc Soc Behav Sci 62(2):263–267. https://doi.org/10.1016/j.sbspro.2012.09.042
18. Erin O, Uwuigbe U, Eriabie S, Uwuigbe O, Omoike O (2019) Does enterprise risk management impact accounting quality? Evidence from the Nigerian financial institutions. Invest Manag Financ Innov 16(4):1–15. https://doi.org/10.21511/imfi16(4).2019.02
19. Erin O, Uwuigbe U, Eriabie S, Uwuigbe O (2019) Risk governance and firm performance in the Nigerian's financial sector. In: Proceedings of the 33rd international business information management association conference, IBIMA 2019: Education Excellence and Innovation Management Through Vision 2020. https://ibima.org/conference/33rd-ibima-conference
20. Li Q, Wu Y, Ojiako U, Marshall A, Chipulu M (2014) Enterprise risk management and firm value within China's insurance industry. Acta Commercii 14(1):1–10. https://doi.org/10.4102/ac.v14i1.198
21. Erin O, Osariemen A, Olojede P, Ajetunmobi O, Usman T (2018) Does risk governance impact bank performance? Evidence from the Nigerian Banking Sector. Acad Account Financ Stud J 4(1):1–14
22. Institute of Risk Management (IRM) (2014) Cyber-risk: resources for practitioners. https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf
23. Baxter R, Bedard J, Hoitash J, Yezegel A (2013) Enterprise risk management program quality: determinants, value relevance, and the financial crisis. Contemp Account Res 4(2):34–54. https://doi.org/10.1111/j.1911-3846.2012.01194.x
24. Robinson R (2017) Risk governance: the true secret weapon of cybersecurity. https://securityintelligence.com/risk-governance-the-true-secret-weapon-of-cybersecurity/
25. International Risk Governance Council (IRGC) (2005) White paper no. 1: risk governance—towards an integrative approach. International Risk Governance Council (IRGC), Geneva. https://irgc.org/risk-governance/irgc-risk-governance-framework
26. Liebenberg A, Hoyt R (2003) The determinants of enterprise risk management: evidence from the appointment of chief risk officers. Risk Manag Insur Rev 6(1):37–52. https://doi.org/10.1111/1098-1616.00019
27. Dickinson G (2001) Enterprise risk management: its origins and conceptual foundations. Geneva Pap Risk Insur Issues Pract 26(3):360–366. https://doi.org/10.1111/1468-0440.00121
28. Rahim S, Mahat F, Nassar A, Yahya M (2015) Re-thinking: risk governance? Proc Econ Finance 31(2):689–698. https://doi.org/10.1016/S2212-5671(15)
29. McShane M, Nair A, Rustambekov E (2011) Does enterprise risk management increase firm value? J Account Audit Finance 16(4):641–658. https://doi.org/10.1177/2F0148558X11409160
30. Beasley M, Clune R, Hermanson D (2005) Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. J Account Public Policy 24(1):521–531. https://doi.org/10.1016/j.jaccpubpol.2005.10.001
31. Standard & Poor (2005) Evaluating the risk management practices of insurance companies. Standard and Poor, New York. https://www.actuaries.org.uk/system/files/field/document/insurancecriteria.pdf
32. Nocco B, Stulz R (2006) Enterprise risk management: theory and practice. J Appl Corp Finance 18(1):8–20. https://doi.org/10.1111/j.1745-6622.2006.00106.x
33. Arumona J, Erin O, Onmonya L, Omotayo V (2019) Board financial education and firm performance: evidence from the healthcare sector in Nigeria. Acad Strateg Manag J 18(4):1–18
34. Yong H (2017) Enterprise risk management in Malaysia: a case study. Retrieved from https://www.researchgate.net/publication/317076215_
35. Kleffner A, Lee R, McGannon B (2003) The effect of corporate governance on the use of enterprise risk management: evidence from Canada. Risk Manag Insur Rev 6(1):53–73. https://doi.org/10.1111/1098-1616.00020
36. Daud W, Yazid A, Hussin M (2010) The effect of chief risk officer (CRO) on enterprise risk management (ERM) practices: evidence from Malaysia. Int Bus Econ Res J 9(11):55–64. https://doi.org/10.5539/ijbm.v6n12p205
37. Boholm A, Corvellec H, Karlsson M (2014) The practice of risk governance: lessons from the field. J Risk Res 15(1):1–20. https://doi.org/10.1080/13669877.2011.587886
38. Hoyt R, Liebenberg A (2011) The value of enterprise risk management. J Risk Insur 78(4):795–822. https://doi.org/10.1111/j.1539-6975.2011.01413.x
39. Eckles D, Hoyt R, Miller S (2014) The impact of enterprise risk management on the marginal cost of reducing risk: evidence from the Insurance Industry. J Bank Finance 43(2):247–261. https://doi.org/10.1016/j.jbankfin.2014.02.007
40. Peters S, Miller M, Kusyk S (2011) How relevant is corporate governance and corporate social responsibility in emerging markets? Corp Gov 11(4):429–445. https://doi.org/10.1108/14720701111159262
41. Ellul A, Yerramilli V (2012) Stronger risk controls, lower risk: evidence from US bank holding companies. J Finance 68(5):1757–1803. https://doi.org/10.1111/jofi.12057
42. Decker A, Galer D (2010) Getting the focus on enterprise risk management right (Online). http://community.rims.org/RIMS/RIMS/Community/Resources/ViewDocument/.Default.aspx?DocumentKey=47b61f84-4341-47f9-8fdc-2dd50d64ac29
43. Okoye L, Adetiloye K, Erin O, Evbuomwan G (2017) Impact of banking consolidation on the performance of the banking sector in Nigeria. J Internet Bank Commerce 22(1):1–16

44. Rochette M (2009) From risk management to enterprise risk management (ERM). J Risk Manag Financ Inst 2(4):394–408
45. Ame J, Arumona J, Erin O (2017) The impact of ownership structure on firm performance: evidence from listed manufacturing companies in Nigeria. Int J Account Finance Inf Syst 1(1):293–305
46. Campa J, Kedia S (2002) Explaining the diversification discount. J Finance 57(4):1731–1762. https://doi.org/10.1111/1540-6261.00476
47. Uwuigbe U, Erin O, Uwuigbe O, Igbinoba E, Jafaru J (2017) Ownership structure and financial disclosure quality: evidence from listed firms in Nigeria. J Internet Bank Commerce 22(8):1–12. https://doi.org/10.22495/cocv14i4art8
48. Ilaboya O, Ohiokha I (2016) Firm age, size and profitability dynamics: a test of learning by doing and structural inertia hypotheses. Bus Manag Res 5(1):29–39. https://doi.org/10.5430/bmr.v5n1p29
49. Erin O, Ogueyungbo O, Ogundele I, Ogundele O (2017) Effect of the business model and strategic growth factors on organization value creation. J Knowl Manag Econ Inf Technol 7(4):1–17
50. Majumdar SK (1997) Impact of size and age on firm-level performance: some evidence from India. Rev Ind Organ 12:231–241. https://doi.org/10.1023/A:1007766324749
51. Papatogonas E (2007) Financial performance of large and small firms: evidence from Greece. Int J Financ Serv Manag 2(1):14–20. https://doi.org/10.1504/IJFSM.2007.011668
52. Golshan N, Rasid S (2012) Determinants of enterprise risk management (ERM) adoption: an empirical analysis of Malaysian Public Listed Firms. Int J Soc Hum Sci 6(1):119–126. https://doi.org/10.5281/zenodo.1079700
53. Dabari J, Saidin S (2015) Determinants influencing the implementation of enterprise risk management in the Nigerian banking sector. Int J Asian Soc Sci 5(12):740–754. https://doi.org/10.18488/journal.1/2015.5.12/1.12.740.75
54. Obalola M, Akpan T, Abass O (2014) The relationship between enterprise risk management (ERM) and organisational performance: evidence from Nigerian Insurance Industry. Res J Finance Account 5(14):102–126
55. Ugwuanyi U, Imo G (2014) Enterprise risk management and performance of Nigeria's brewery industry. Dev Country Stud 2(10):60–67
56. Dowling J, Pfeffer J (1975) Organizational legitimacy: social values and organizational behavior. Pac Soc Rev 18(1):122–136. https://doi.org/10.2307/1388226
57. Deegan C (2002) The legitimising effect of social and environmental disclosures—a theoretical foundation. Account Audit Account J 15(3):282–311. https://doi.org/10.1108/09513570210435852
58. Andersen T (2009) Effective risk management outcomes: exploring effects of innovation and capital structure. J Strategy Manag 2(4):352–379. https://doi.org/10.1108/17554250911003845
59. Flora C, Leoni G (2016) Enterprise risk management (ERM) and firm performance: the Italian Case. Br Account Rev 3(1):36–50. https://doi.org/10.1016/j.bar.2016.08.003
60. Corbett C, Kirsch D (2001) International diffusion of ISO 14000 certification. Prod Oper Manag 10(3):327–342. https://doi.org/10.1111/j.1937-5956.2001.tb00378.x
61. Sharma U, Lawrence S, Lowe A (2010) Institutional contradiction and management control innovation. A field study of total quality management practices in a privatized telecommunication company. Manag Account Res 21(4):251–264. https://doi.org/10.1016/j.mar.2010.03.005
62. Arena M, Arnaboldi M, Azzone G (2012) The organizational dynamics of enterprise risk management. Account Organ Soc 35(7):659–675. https://doi.org/10.1016/j.aos.2010.07.003
63. Mikes A, Kaplan R (2014) Managing risks: towards a contingency theory of enterprise risk management. Working paper, Harvard Business School. https://www.hbs.edu/faculty/Publication%20Files/13-063_5e67dffe-aa5e-4fac-a746-7b3c07902520.pdf
64. Shima N, Mahmood Z, Happy M, Akbar A (2013) Enterprise risk management and performance in Malaysia. Interdiscip J Contemp Res Bus 5(1):670–707
65. Okoye L, Adetiloye K, Erin O, Evbuomwan G (2016) Impact of banking consolidation on the performance of the banking sector in Nigeria. In: Proceedings of the 28th international business information management association conference, IBIMA 2016: Innovation Management, Development Sustainability and Competitive Economic Growth Through Vision 2020. https://ibima.org/conference/28th-ibima-conference/
66. Cavezzali E, Garddenal G (2015) Risk governance and performance of the Italian banks: an empirical analysis. Working paper 8. Department of Management, Università Ca' Foscari Venezia
67. Aebi V, Sabato G, Schmid M (2011) Risk management, corporate governance, and bank performance in the financial crisis. J Bank Finance 32(2):3213–3226. https://doi.org/10.1016/j.jbankfin.2011.10.020
68. Arnold V, Benford T, Canada J, Sutton S (2011) The role of strategic enterprise risk management and organizational flexibility in easing new regulatory compliance. Int J Account Inf Syst 12(3):171–188. https://doi.org/10.1016/j.accinf.2011.02.002
69. Securities and Exchange Commission (SEC) (2015) Corporate governance code for financial institutions. Retrieved from https://sec.gov.ng/regulation/rules-codes/
70. Creswell J (2014) Research design: qualitative, quantitative and mixed method approaches, 2nd edn. Sage Publications, California
71. Ojeka S, Ben-Caleb E, Ekpe E (2017) Cybersecurity in the Nigerian banking sector: an appraisal of audit committee effectiveness. Int Rev Manag Market 7(2):340–346

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.