CHALLENGES AND RECOMMENDATIONS FOR INFORMATION GOVERNANCE IN THE NIGERIA BANKING SECTOR

ABSTRACT

Aims: The article provides an overview of the Nigerian banking industry, highlighting its regulation by the Central Bank of Nigeria (CBN) and the role of information governance (IG) in enhancing the industry's robustness. Despite being recognized as one of the top performers in Africa, there are inconsistencies in information governance, particularly in data management.
Place of Study: The case study of Capital One showed that implementing appropriate governance policies could have either entirely mitigated the attack or reduced the time the hackers had unauthorized access, minimizing the attack's impact on the organization.
Methodology: The study employed a mixed-methods approach to explore the feasibility of implementing an Information Governance Framework (IGF) in the financial sector. The quantitative data collected from Nigerian Deposit Insurance Corporation (NDIC), the regulator of banking industry in Nigeria revealed that implementing IG programs is crucial for profitability in the banking industry.
Results: The study concludes that effective IG depends on formalized structures, accountability, privacy, ethics, transparency, monitoring, compliance, and suitability.
Conclusion: Therefore, with 95% confidence, it can be stated that IG policies does not contribute to mitigating data breaches in the Nigerian banking industry and improving profitability. The study has shown that financial institutions can utilize information governance to mitigate data breaches and increase profits. While data breaches remain a real threat, banks can leverage IG policies to enhance profitability by safeguarding their assets. As a result, Nigerian banks must remain vigilant and address any changes within their business infrastructure to mitigate risks and protect sensitive data using appropriate IG policies and standards.

Keywords: Nigeria, Banking, Financial Industry, Information Governance, Technology, data breaches, governance, customer information, and data privacy

1. INTRODUCTION

According to Uchenna Okoye et al. (2020), the Nigerian banking industry is highly regarded as one of the top performers in Africa. The industry is regulated by the Central Bank of Nigeria (CBN), which serves as the apex bank and enforces policies that ensure compliance with financial service regulations to safeguard stakeholders' interests (Central Bank of Nigeria, 2007). Due to the nature of banks' services, they collect extensive customer data for various purposes, as highlighted by Ohiani (2021). The CBN also oversees information-related matters to promote ethical practices and conformity with international data management standards (Central Bank of Nigeria, 2007). The banking industry in Nigeria utilizes customer data to develop products, create policies, design services, and anticipate emerging trends and advancements (Ohiani, 2021).

According to Deloitte (2021), the financial industry is undergoing significant changes in the global business environment. However, financial companies are well-positioned to manage critical issues while maintaining profitability. The banking industry is driving transformation across other global economic sectors, making a significant impact beyond financial services delivery (Deloitte, 2021). For instance, a product like a mobile phone involves coordination between organizations in different countries, requiring a robust financial system to facilitate timely payments and smooth transactions to support all other aspects of the business (Uchenna Okoye et al., 2020). A robust financial system is also critical when governments and organizations

UNDER PEER REVIEW

engage in business with one another (Deloitte, 2021). It becomes increasingly vital to safeguard financial assets held by banks worldwide to prevent fraud or cracks in the system that could lead to a collapse as the global economic outlook turns bearish. Information governance (IG) is crucial in enhancing the robustness of any industry, including the banking sector (Uchenna Okoye et al., 2020).

For years, Nigerian banks have relied heavily on physical business offices to provide banking services and conduct operations, with customer information stored in hard copy in safe and filing cabinets in business branches nationwide. However, with the advent of technology, banks have acquired digital banking solutions to meet customer and shareholder expectations (FirstBank, 2023). Business data is now stored electronically and kept in shared folders. Despite these advancements and recognition as one of the best in Nigeria, there are inconsistencies in information governance, especially in data management (Uchenna Okoye et al., 2020). For example, when a customer signs up for a service, data is collected for "Know Your Customer (KYC)" purposes. However, if the same customer enrolls in another service, most of the previously collected data is required again, leading to duplication within the bank (Uchenna Okoye et al., 2020).

1.1 Research Questions

The study seeks to leverage information governance (IG) to minimize data breaches in the banking sector, enhancing profitability. With the growth of the banking industry comes the accumulation of more data, which necessitates strengthening IG policies to reduce data breaches and improve competitiveness. Therefore, the research questions and hypotheses center on how IG policies can minimize data breaches and promote the industry's performance. The research question, Ho, and Hα are presented below:

Research Question: Can implementing Information Governance (IG) policies effectively reduce data breaches in the banking industry and ultimately lead to improved profitability?

1.2 Research Hypotheses

Data breaches are identified as the *dependent variable*, and Information governance policies are identified as *the independent variable*.

Ho – Information Governance policies do not impact mitigating data breaches in the banking industry to enhance profitability.

Hα– IG policies are a contributing factor to mitigating data breaches in the banking industry, leading to an improvement in profitability.

2. LITERATURE REVIEW

The literature review examines and proposes solutions to the banking industry's information governance challenges. The review will document recommendations suggested by researchers to tackle these challenges, practical applications of interventions, and empirical evidence of their effectiveness. A robust evaluation design will be used to provide specific findings. Hence, 18 scholarly peer-reviewed papers using different research methodologies were analyzed to gather information, exploring various aspects of information governance challenges that impact the banking industry.

2.1 Technology Innovation in the Nigerian banking system: Prospects and Challenges

The use of technology in the banking industry has dramatically transformed how banks operate. It has brought various benefits, such as improved efficiency, reduced costs, and enhanced customer experience (Ohiani, 2021). The article explores various technological innovations in the Nigerian banking system, such as mobile banking, internet banking, and electronic payment systems. The author argues that these innovations have been crucial in enhancing the accessibility and convenience of banking services in Nigeria, particularly in rural areas where physical branches are often scarce (Ohiani, 2021). However, the article also highlights some challenges associated with technology innovation in the Nigerian banking system. These challenges include inadequate infrastructure, a low level of digital literacy among the population, and cybersecurity threats. The author notes that these challenges could hamper the growth of the banking sector in Nigeria if not addressed effectively. The article concludes by emphasizing the need for a comprehensive approach to technology innovation in the Nigerian banking system (Ohiani, 2021). This approach should involve investment in infrastructure, education, and training of bank employees and customers and implementing robust cybersecurity measures (Ohiani, 2021).

2.2 Impact of Corporate Governance on Nigerian Commercial Banks

The authors investigate the impact of corporate restructuring on various financial performance indicators such as return on assets (ROA), return on equity (ROE), and net interest margin (NIM). The study

UNDER PEER REVIEW

utilizes a sample of six commercial banks that have undergone corporate restructuring in Nigeria, and data is collected for ten years (Uchenna Okoye et al., 2020). The authors use panel data regression analysis to examine the impact of corporate restructuring on financial performance. The study's findings suggest that corporate restructuring positively and significantly impacts financial performance indicators such as ROA, ROE, and NIM (Uchenna Okoye et al., 2020). The study shows that commercial banks that undergo corporate restructuring tend to have higher financial performance levels than those that do not (Uchenna Okoye et al., 2020). The article provides a detailed explanation of the corporate restructuring process and its potential benefits for commercial banks. The authors also highlight some challenges that may arise during the restructuring process, such as the cost of restructuring and employee resistance (Uchenna Okoye et al., 2020).

2.3 Information Governance Standards in the Banking Sector

The proliferation of data collection activities across the global landscape, undertaken by individuals, businesses, and governments, has revealed that Information Governance (IG) is critical for ensuring information systems security and proper functioning (Faria et al., 2013). Thus, to investigate the impact of IG on the financial industry, 13 banks from Hong Kong, Brazil, and the United States were studied using a multiple-case analysis approach. The study hypothesized that an Information Governance Framework (IGF) could facilitate the implementation of IG in the financial industry and that financial institutions need to consider various elements to manage the industry's complexities (Faria et al., 2013). The study collected data from interviews with bank executives and information from bank websites and trade journals. The findings indicate that the effectiveness of IG depends on each institution's level of maturity and decision-making processes. Consequently, the study proposes a new notion of IG to establish acceptable practices for banks, which could help to mitigate operational risks, reduce costs, and optimize organizational performance (Faria et al., 2013).

2.4 Information Governance Challenges and Global Inequalities in Cyber Capacity Building

The proliferation of IT infrastructure is transforming the global development landscape, with the internet and data exchange facilitating unprecedented global collaboration (Calderaro & Craig, 2020). Consequently, the rising demand for the Internet drives the need to enhance cyber capabilities for organizations, businesses, and governments worldwide. Organizations must boost their cyber capacity to establish globally acceptable governance practices that augment security plans and safeguard assets (Calderaro & Craig, 2020). A quantitative study method was used to identify the critical factors that hinder governments' efforts to enhance their cyber capabilities. The study's findings challenge the recommendations of standard information management practices that suggest building cyber abilities based on environmental realities such as threats, standards, ideals, and politics (Calderaro & Craig, 2020). Instead, the study recommends that decision-makers support the development of robust cyber capabilities that can thwart attacks through education and relevant technical skills (Calderaro & Craig, 2020).

2.5 The Efficiency of Information Security Governance in the United States Banking Sector

The current conventional Information Security Governance (ISG) frameworks need to be revised to address the global ecosystem's growing threat (Tanoh, 2022). Therefore, organizations must develop new, contemporary enterprise-specific ISG frameworks to enhance cyber defenses and mitigate threats (Tanoh, 2022). The study hypothesized that the strategic alignment of ISG with business goals positively impacts value-delivery procedures. The research method was quantitative and non-experimental, and it aimed to investigate the relationship between strategic alignment and value delivery in the context of the significance of ISG (Tanoh, 2022). A questionnaire was distributed to 150 information governance professionals from various banks in the United States. Simple linear regression and analysis of variance were employed to explore the connections between strategic alignment and value delivery (Tanoh, 2022). The results indicate that implementing a stakeholder approach with new cyber-oriented standards could enhance the effectiveness of ISG within the U.S. banking sector.

2.6 Incorporating Data Governance Frameworks in the Financial Sector

Financial institutions need help managing the vast amounts of data they accumulate, leading to a growing realization of the importance of implementing Data Governance frameworks in their operations (Randhawa, 2019). Such a framework can enhance operations, facilitate faster decision-making, and improve risk and fraud management in the financial industry (Randhawa, 2019). However, corporate data managers often require assistance with implementing these frameworks. This multiple case study focuses on successful corporate data managers at several banks in the United States who implemented data governance frameworks to reduce operational risks and costs (Randhawa, 2019). The study involved seven corporate data managers from three banks in New York and North Carolina, using the servant leadership conceptual framework. Through qualitative analysis of individual experiences, the study identified strategies for addressing specific

UNDER PEER REVIEW

business problems. The results of this research can contribute to positive social change by supporting effective data management strategies in banks, improving data quality and security, and enhancing decision-making to benefit customers (Randhawa, 2019).

2.7 Information Technology Governance Trends in Financial Industry

The financial sector recognizes the critical role of Information Governance (IG) in supporting, sustaining, and shaping organizational strategies, both new and existing. A practical IG framework helps organizations align their IT structures with their strategy, culture, and mission (Pereira et al., 2014). This study analyzes several case studies to identify challenges and opportunities in implementing IG practices in the financial industry. Design science research is employed as the research methodology to investigate the increasing popularity of IG and its relation to the information system domain. The study demonstrates the usefulness of design science research in capturing the complexity of IG patterns in the financial sector (Pereira et al., 2014). The case studies provide insights into good practices in the IG sector and highlight the government's role in enforcing adequate IG standards in the financial sector.

2.8 Possible Consequence of Information Governance Breaches in the Financial Sector

The financial industry has embraced peer-to-peer tracking of ownership for financial assets, which has garnered widespread attention. This application involves recording essential statistics in a database for practical evaluation (Yermack, 2017). However, stock compensation manipulation has become increasingly challenging, and transparent liquidation of client positions may make a periodic intervention in information governance attractive at the expense of their intervention (Yermack, 2017). The evolution of information governance in the financial sector may vary with the emergence of new technologies such as blockchain and cryptocurrency. As a result, additional governance policies will need to be implemented to address the potential implications of these changes on the industry and establish a security policy for the entire financial sector (Yermack, 2017).

2.9 Embracing Information Technology Governance to Boost Financial Performance

Adopting Information Governance (IG) in organizations results in better financial performance and higher investment returns than their peers (Lunardi et al., 2014). The performance of an organization is influenced by the implementation of IG before and after its adoption, which reflects changes and relevance within the organization and ensures proper governance management. IG controls the organization strategically, harnesses the value of IT, and mitigates and controls risks (Lunardi et al., 2014). To achieve this, organizations use COBIT and ITIL as adequate IG drivers to improve organizational performance and make gains. However, new challenges emerge as an organization grows and becomes more stable. Management is crucial for sustaining, supporting, and growing the business, while focusing entirely on IG to save money instead of following it can be detrimental (Lunardi et al., 2014).

2.10 The Function of Board Structure in the Financial Performance Executing Information Governance

In the financial sector, implementing IG is crucial to prevent mismanagement and failures within organizations. Mismanagement can weaken the structure and financial management of a robust industry like finance (Handa, 2018). To thrive in an open environment, corporations must establish suitable mechanisms and governance, including IG (Handa, 2018). By implementing IG, organizations can enhance firm and shareholder performance, improving accountability and values for stakeholders. When mismanagement occurs, stakeholders often reorganize IG practices and norms to establish a functioning organization. This paper uses panel regression to analyze the effectiveness of board performance in implementing adequate IG policies (Handa, 2018).

European Policies for Environmental, Social, and Governance in the Banking Sector

Policymakers across the globe are emphasizing the creation of frameworks and regulations that promote stability, robustness, equity, and sustainability in the financial system. This trend is particularly prevalent in Europe, with a shift in perspective from the previously accepted view that firms, including banks, were primarily focused on maximizing profits while maintaining a level of ethics and principles. The current view is that firms should also consider the impact of their actions on the ecosystem of participants affected by their operations, such as their employees, customers, and local communities (Bruno & Legasio, 2021). The hypothesis that environmental and social policies and corporate governance have a direct correlation with a bank's profitability is supported by the positive impacts of implementing ESG policies, which can drive customer acquisition, retention, and profits. Countries like Italy, France, and Denmark have policies that require firms, asset managers, and investment funds to disclose all their holdings, which promotes

UNDER PEER REVIEW

transparency and trust in the system (Bruno & Legasio, 2021). Despite the success of ESG policies in finance, there is a need for increased knowledge and awareness of their implementation and benefits.

2.11 Solving Cybercrime with Information Governance

With the rapid evolution of technology, cybercriminals, and hackers have become increasingly sophisticated in their attacks. While the Internet provides many advantages, including globalization and increased collaboration, it has also made governments, organizations, and firms more vulnerable to exploitation (Onwujekwe et al., 2019). Cybersecurity measures are essential to prevent security breaches, data integrity destruction, or information theft. The European Union has introduced regulations, such as the General Data Protection Regulation (GDPR), to combat cybercrime and take action against non-compliant participants (Onwujekwe et al., 2019). In recent years, there has been an increase in journal articles discussing the benefits of implementing a robust data governance program to tackle cybercrime. A robust data governance program involves developing processes, principles, standards, and policies to support data governance and establishing a dedicated team with defined roles, responsibilities, training, and communication plans (Onwujekwe et al., 2019).

2.12 Bank Data Infringement

The July 2019 data breach at Capital One, one of the largest in history, is a case that warrants specific study. Capital One, the fifth-largest bank in the United States and operating in a heavily regulated industry, adhere to recommended data governance procedures, regulations, and standards (Neto et al., 2020). Despite this, the bank's data was still breached, affecting over one hundred million customers (Neto et al., 2020). The attackers used TOR to conceal their identity. They exploited a misconfiguration in the Web Application Firewall (WAF) to send commands to the Amazon Web Services (AWS) metadata service (Neto et al., 2020). They also listed all available AWS S3 Buckets using the "ls" command and copied the contents of all listed S3 buckets into their local server using the "sync" command (Neto et al., 2020). The two areas of control failure were the storage and retrieval of credentials in a secure format (Access Key and Secret ID) and the inability to monitor outbound traffic from the Capital One AWS servers to stop data exfiltration. Recommendations based on this breach include adopting proper compliance controls, upgrading control procedures to keep up with evolving technology, and hiring skilled multidisciplinary professionals instead of avoiding compliance controls (Neto et al., 2020).

General Information Privacy and Protection Laws

Implementing the General Data Protection Regulation (GDPR) in Europe in 2018 spurred the introduction of similar measures in North America (Merrick & Ryan, 2019). In the United States, various acts and legislations have been enacted to safeguard individuals' online privacy, which the Federal Trade Commission enforces in collaboration with eight other federal agencies (Merrick & Ryan, 2019). These measures, such as the Children's Online Privacy Protection Act (COPPA), California Customer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA), establish guidelines and frameworks for organizations to handle customer data, including sensitive information such as Social Security Numbers, Addresses, Phone Numbers, Bank Accounts, etc. Protecting data privacy is just as crucial as information governance, as a breach of privacy can compromise data integrity, leading to financial losses (Merrick & Ryan, 2019). The costs of such breaches to customers and organizations are extensive and include stock price drops, sales, and operational disruptions, legal and settlement fees, system downtime, loss of wages, identity theft, and regulatory fines (Merrick & Ryan, 2019).

Development of the Banking System and Current Challenges

A study on the Kyrgyzstan banking system's post-independence performance presents five distinct stages, each with specific goals and objectives (Aseinov & Karymshakov, 2018). Despite facing unforeseen challenges in recent years, Kyrgyzstan has made significant progress in the last two decades. However, the availability of financial resources is crucial to ensure sustainable economic development. Achieving a thriving financial system requires various economic reforms to address internal and external factors, which may be unpredictable and unrecognized (Aseinov & Karymshakov, 2018). The study presents a chronological account of the banking system's evolution in Kyrgyzstan, detailing the five phases and their corresponding economic conditions. The first phase involved comprehensive and radical economic reforms, while the second was marked by instabilities caused by the Russian crisis and internal banking system deficiencies. The third phase focused on ongoing economic recovery, while the fourth and fifth phases dealt with the global financial crisis and the consequences of external instability (Aseinov & Karymshakov, 2018).

Bridging the Gap between Information Technology and Business in the Banking Sector

UNDER PEER REVIEW

Effective implementation of an information governance framework is critical in bridging the gap between business and IT by considering several factors. Information governance strategies have significantly impacted the banking industry over the last 50 years, focusing on business process improvements (Faria & Simpson, 2013). Banks continuously strive to enhance their performance while optimizing resource utilization and increasing efficiency. The evolution of information technology has enabled banks to explore new environments, offer new products and services, and leverage various delivery channels (Faria & Simpson, 2013). It is important to note that IT has also transformed the industry's product offerings, procedures, and competitive landscape. These changes have led to new business opportunities and altered the industry structure, leading to faster advancements in the banking sector (Faria & Simpson, 2013). As a result, banks can now fulfill customer requests promptly and efficiently, eliminating the long wait times that were once common in the early days of banking (Faria & Simpson, 2013).

Information Security Administration Using ISO/IEC 27001 Standard

The financial industry's standard and primary concerns have been reexamined through the lens of social systems thinking, leading to interdisciplinary studies and essential research findings related to potential motivation, relation to other standards, implementation challenges, practical outcomes, and contextual factors (Bounagui et al., 2019). Some requirements may seem overly theoretical or ambitious, but they provide necessary guidance on what actions should ideally be taken. The organization is responsible for selecting the approach that best aligns with these objectives and goals (Bounagui et al., 2019). The ISO/IEC 27001 standard is particularly useful in developing effective information management practices for organizations, and it remains relevant in achieving significant business outcomes in the current business environment (Bounagui et al., 2019).

Cybersecurity Disclosure in the Banking Sector

Cybersecurity disclosure is crucial in providing potential customers and users with significant insights and knowledge about future cyber risks and how they can be managed (Mazumder & Hossain, 2022). Therefore, to explore the relationship between cyber risk and components such as the size, independence, and gender diversity of the board of directors, this study focused on the board of directors as they are considered critical players in managing cyber risk. The study utilized automated content analysis and applied multiple linear regression procedures to determine the relationship between cyber security disclosure and the board of directors' responsibility (Mazumder & Hossain, 2022). The results show a positive relationship between the independence of the board and the level of cyber security disclosure. These findings can help policymakers and board members make more informed decisions and meet corporate governance guidelines (Mazumder & Hossain, 2022).

Identified Information Governance Challenges

The Capital One case study was analyzed due to the various challenges that resulted in several data breaches in the banking sector, despite the bank's adherence to stringent information governance policies and a sturdy security framework. The following issues were identified as potential causes of the security breach:

Using Unrecognized Networks to Hide Identity

Hackers frequently use URNs (Unrecognized Networks) to mask their identity and gain initial access to an organization's servers. This is often achieved through a user's assumed or guessed password on the server via an FTP (File Transfer Protocol), email, or SSH (Secure Shell) user (Neto et al., 2020) or by exploiting security vulnerabilities in web applications like WordPress, Drupal, or other web applications (Neto et al., 2020).

Exploiting Vulnerabilities in Server Patches

The organization's server may require additional patches to counter attacks from third-party or hackers who can access it remotely and create vulnerabilities in its private server. Implementing adequate information governance (IG) policies can mitigate the risk of attackers gaining unauthorized access to the organization's data. Stakeholders can be critical in shaping the company's structure and processes to enhance profitability (Neto et al., 2020).

Exploiting Misconfigurations in Web Application Firewalls

Improperly configured firewalls can provide a gateway for malicious actors to exploit vulnerabilities and gain unauthorized access. A viable technical solution to this issue is ensuring that all web application firewalls are correctly configured (Neto et al., 2020).

Unauthorized Access to Credentials and Secret Keys

The Capital One data breach involved hackers circumventing the firewall and obtaining administrative account privileges, which enabled them to execute sync commands on AWS. (Neto et al., 2020).

Ability To Run Commands to List and Sync Using Cloud Data Storage

Cloud storage is used by organizations to store their data offsite, reducing the need for onsite data warehousing and lowering storage costs. However, good information governance policies are necessary to prevent unauthorized access and data breaches, such as the pulling out of buckets, and to ensure adequate firewall protections. The Capital

UNDER PEER REVIEW

One data breach is an example of inadequate cloud storage security, specifically the misconfiguration of Amazon Web Services' S3 (Neto et al., 2020).

2 METHODOLOGY

The research methodology employed in this study is mixed methods, comprising a case study of secondary data and quantitative analysis of secondary data to test the hypothesis. The case study involved an exhaustive examination of the technical procedures involved in the attack, the conditions that facilitated the breach, and the relevant regulations (Neto et al., 2020). The quantitative analysis utilized data from 13 banks in Hong Kong, Brazil, and the United States to evaluate the impact of IG on the financial industry. The study explored the feasibility of implementing an Information Governance Framework (IGF) in the financial sector and whether financial institutions should consider various factors to manage the industry's complexities (Faria et al., 2013). Data was collected through interviews with senior bank executives and by analyzing bank websites and trade journals. The data analysis was conducted using computer-assisted qualitative data analysis software (CAQDAS), specifically the NVivo version 9 from QSR Software (Faria et al., 2013).

In addition, the Deposit Insurance System (DIS) in Nigeria that is managed by the Nigeria Deposit Insurance Corporation (NDIC), a statutory organization created by NDIC Act No. 16 of 2006 is another source of data used to corroborate the hypotheses in the study. The NDIC's data on cybercrime and banking industry is used to assess the potency of the sector’s information governance (IG). The data are of quarterly frequency ranging from 2011Q1 to 2021Q1 as extracted from various sources. We employed an Ordinary Least Square (OLS) estimating technique to validate the hypotheses in the study.

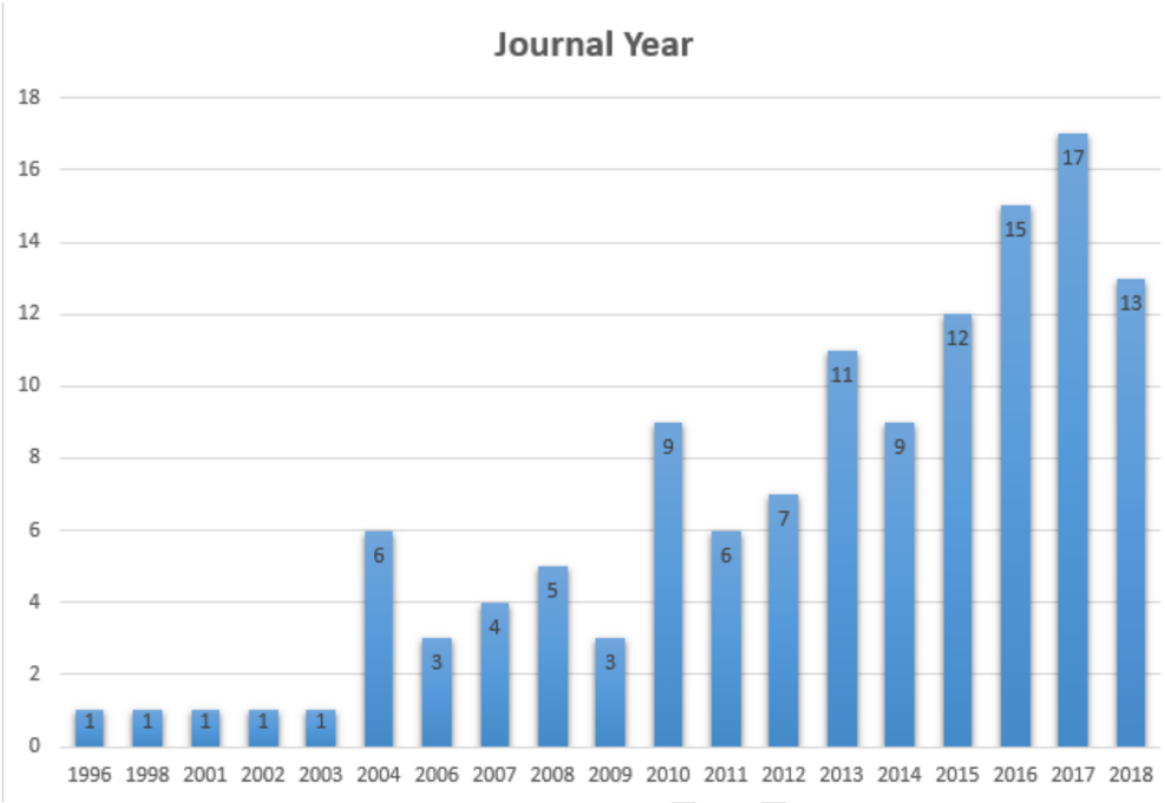
3. RESULTS AND DISCUSSION

3.1 Data Analysis

After analyzing the quantitative data, it was found that the null hypothesis, which states that "information governance policies do not contribute to mitigating data breaches in the banking industry to improve profitability," was rejected. Although IG policies may not eliminate data breaches, they can reduce the financial strain and loss on organizations caused by such incidents. Moreover, the interview with 16 executives from 13 banks revealed that a good IG policy is essential in preventing data breaches, as all respondents answered in the affirmative. Therefore, our research supports the alternate hypothesis, which suggests that implementing IG programs is crucial for profitability in the banking industry. While limited quantitative research exists on the direct, measurable impact of IG programs on profitability, the literature suggests that research on measuring the impact of IG programs is steadily growing, as indicated in Figure 1.

UNDER PEER REVIEW

Figure 1: *Journal Articles About the Impact of IG by Year*



Source: Onwujekwe et. al., 2019.

After analyzing the Capital One case study, it is evident from the literature that implementing good governance policies could have either entirely mitigated the attack or reduced the time the hackers had unauthorized access; this could have resulted in minimizing the attack's impact on the organization. The attack had multiple stages, as indicated in Figure 2 below.

Figure 2: *Visualization of the Capital One Data Breach*

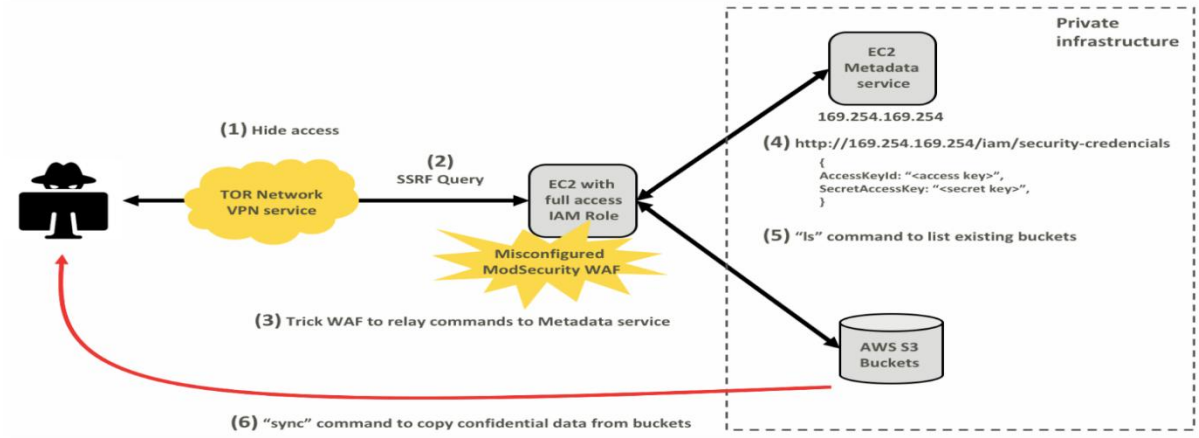


Figure 2: Diagram of the attack: Capital One case study

Source: Neto et al., 2020.

According to the literature, many governing bodies and policymakers are implementing IG programs in their organizations, including governments worldwide. The number of bodies responsible for ensuring compliance with the latest IG frameworks and standards is also growing steadily. Data privacy acts are being enacted with legal implications to ensure the proper handling of sensitive customer information. In another study, high-ranking executives from thirteen different banks worldwide were interviewed to understand their position, willingness, and strategy to implement an IG framework at their bank (Faria et al., 2013). The results are summarized as shown in the table below.

Figure 3: *List of Executives Interviewed*

Executive		Interview				Bank	
#	Position	Date	City	Idiom	Recorging Time	Code	Country of Origin
1	Director	Oct/2011	Brasília	P	58:36	BRA1	Brazil
2	Director	Oct/2011	Brasília	P	54:55	BRA1	Brazil
3	Executive Director	Oct/2011	Brasília	P	66:30	BRA2	Brazil
4	LA Chairman	Jan/2012	São Paulo	P	71:13	USA1	United States
5	Director of IT	Mar/2012	São Paulo	P	56:37	BRA3	Brazil
6	Senior VP	Dec/2011	Hong Kong	E	57:15	HKG1	China
7	Head of IT	Dec/2011	Hong Kong	E	26:50	HKG2	Japan
8	General Manager	Dec/2011	Hong Kong	E	37:01	HKG3	China
9	CIO AP	Dec/2011	Hong Kong	E	18:34	HKG4	France
10	Head of IT	Dec/2011	Hong Kong	E	38:57	HKG5	Germany
11	LA Technology Head	Jan/2012	Fort Lauderdale	P	55:33	USA1	United States
12	CIO	Jan/2012	New York	E	40:32	USA2	United States
13	COO	Jan/2012	New York	E	37:03	USA3	United Kingdom
14	Managing Director	Jan/2012	New York	E	36:34	USA1	United States
15	Managing Director	Jan/2012	New York	E	30:27	USA4	United States
16	Executive Director	Jan/2012	New York	P	48:50	USA5	United States

Source: Faria et al., 2013

A quantitative study found that better governance of banking information would result in greater efficiency of operations, minimized risks, and better use of accurate data. The leading factors of IG frameworks implemented at banks were formalized structures, accountability, privacy, ethics, transparency, monitoring, compliance, and suitability (Faria et al., 2013). The analysis was conducted using computer-assisted qualitative data analysis software (CAQDAS), specifically NVivo version 9 from QSR Software. The study concluded that effective IG depends on each institution's level of maturity and decision-making. Therefore, a, new notion for IG is proposed to define acceptable IG practices for banks to curb operating risks, reduce expenses, and optimize the organization's performance.

3.2 Validation of our Hypotheses

We estimated and analyzed the OLS estimator to validate the null hypothesis that Information Governance policies do not impact mitigating data breaches in the banking industry to enhance profitability. The dependent variable in the first model is Return on Assets (ROA), while the regressor in the second model is Return on Equity (ROE) as a measure of profitability of banking sector.

The result in Figure 4 depicts the observed relation between Information Governance policies do not impact mitigating data breaches in the banking industry to enhance profitability. In the model, the findings show that there is a negative and statistically significant relationship (P = .01) between data breaches (DBreach)) and ROA. It shows that a 1% increase in data breaches in Nigeria leads to approximately 0.44 percent decrease in return on assets. In other words, this implies that as the incidence of data breaches increases, banking profitability in terms of ROA decreases. Accordingly, it is expectedly found that human capital development (HCD), when all other factors are held constant, has a positive and statistically significant impact on ROA at p=.05%. This suggests that the profitability of the banking industry is positively impacted by HCD. That is human capital does positively influence efficiency of banking sector in Nigeria. Last, the institutional factor as a measure of information governance (InfoGov) shows a negative but not statistically significant impact on ROA. This implies that the level of information governance negatively influences banking profitability in Nigeria, ceteris paribus.

Thus, the empirical evidence implies that the null hypothesis cannot be rejected which is contrary to the findings from the systematic review.

Figure 4: Information Governance and Profitability

Linear regression

lnROA	Coef.	St.Err.	t-value	p-value
lnDBreach	-0.436	0.075	-5.79	0.000
lnHCD	1.909	1.209	1.58	0.022
InfoGov	-2.254	1.854	-1.22	0.231
Constant	-0.762	1.732	-0.44	0.663

UNDER PEER REVIEW

Mean dependent var	0.53	SD dependent var	0.693
R-squared	0.464	Number of obs	43
F-test	11.248	Prob > F	0
Akaike crit. (AIC)	70.722	Bayesian crit. (BIC)	77.767

*** p<.01, ** p<.05, * p<.1

To validate the hypothesis the null hypothesis that InfoGov policies are a contributing factor to mitigating data breaches in the banking industry, leading to an improvement in profitability, we interacted DBreach and InfoGov to generate a variable DBreach_InfoGov which is used in the model to its impact on banks' profitability which is proxied by return on equity (ROE) and the result depicts in Figure 5.

In the model, the findings show that there is a negative and statistically significant relationship (P=.01) between DBreach_InfoGov and ROE. It shows that as the incidence of data breaches due to poor information governance increases, banking profitability in terms of ROE decreases. Consequently, the empirical evidence implies that the null hypothesis cannot be rejected which implies that IG policies are a contributing factor to mitigating data breaches in the banking industry, leading to an improvement in profitability.

Figure 5: IG policies and Return on Equity (ROE)

Linear regression

lnROE	Coef.	St.Err.	t-value	p-value
DBreach_InfoGov	-0.201	0.054	-3.74	0.001
lnHCD	2.447	1.372	1.78	0.082
lnYUN	-0.269	0.321	-0.84	0.406
Constant	3.223	1.143	2.82	0.007
Mean dependent var	2.715		SD dependent var	0.761
R-squared	0.284		Number of obs	44
F-test	5.301		Prob > F	0.004
Akaike crit. (AIC)	93.099		Bayesian crit. (BIC)	100.236

*** p<.01, ** p<.05, * p<.1

4. Discussion

Our research focuses on the challenges facing information governance (IG) and how practical recommendations can help the banking industry overcome data breaches and increase profitability. We conducted a literature review of 18 peer-reviewed journals and found that the global ecosystem is shifting, increasing data collection by individuals, businesses, and governments (Faria et al., 2013). The adoption of data privacy governance and general data protection regulations has been more prevalent in Europe than in the United States (Bruno & Legasio, 2021).

To protect enterprise information, organizations need to embrace international standards such as ISO/IEC 27001 for information security management (Bounagui et al., 2019). Failure to adopt such regulations can result in critical outcomes such as a drop in stock price, sales, and operation disruption, leading to legal costs, loss of wages, and unnecessary regulatory fees (Wang et al., 2019). IG can help mitigate data breaches from cyber attacks (Calderaro &

UNDER PEER REVIEW

Craig, 2020). Faria and Simpson (2013) discussed the importance of bridging the gap between business and information technology in the banking industry, which affects governance.

Aseinov and Karymshakov (2018) examined the evolution of the banking economy in Kyrgyzstan and used five stages to highlight the global financial crisis and several external challenges in the baking industry. Adopting IG has improved financial performance in many ways (Neto et al., 2020). The Lunardi et al. (2014) study showed that companies become more robust after adopting IG, adapting quickly to the latest IG standards to compete. Incorporating a data governance framework in the banking industry can result in positive social changes (Handa, 2018). If banks adopt the IG framework correctly, they can retain more accurate data, minimize potential data breaches, and guarantee solid consumer data protection (Tanoh, 2022). Quality data can position an organization to compete and profit (Randhawa, 2019).

Relying our empirical models, we found a negative and statistically significant relationship (P = .01) between data breaches (DBreach)) and ROA. In other words, the incidence of data breaches is likely to lead to a reduction in the profitability (ROA) of banking in Nigeria. Similarly, a negative and statistically significant relationship (P=.01) was discovered between DBreach_InfoGov and ROE. This shows that as the incidence of data breaches due to poor information governance increases, banking profitability in terms of ROE decreases. Consequently, the empirical evidence implies that the null hypothesis cannot be rejected which implies that IG policies are a contributing factor to mitigating data breaches in the banking industry, leading to an improvement in profitability. Accordingly, we found that human capital development (HCD), when all other factors are held constant, has a positive and statistically significant impact on ROA at p=.05%. That is human capital does positively influence efficiency of banking sector in Nigeria. Last, the institutional factor as a measure of information governance (InfoGov) shows a negative but not statistically significant impact on ROA. This implies that the level of information governance negatively influences banking profitability in Nigeria, ceteris paribus.

Recommendation

It is crucial to keep watch and address any change within the business enterprise infrastructure to mitigate risks and safeguard sensitive data (Li et al., 2019). As a result, we make the following recommendations to address the challenges identified for the data breach at Capital One Bank.

Using Unrecognized Networks to Hide the Identity

To prevent attacks from untrusted networks and to protect against data leaks, it is crucial to list and block all malicious Internet Protocols (IPs) and external websites. Incoming traffic from such domains or IPs should be blocked to prevent attackers from hiding their identities. Additionally, external service providers' requests should be scanned at the firewall. Any unused ports should also be scanned and closed automatically if found to be open. It is essential to take these precautions to ensure information security (Neto et al., 2020).

Exploiting Vulnerabilities in Server Patches

Preventive controls such as well-configured WAF and vulnerability scanners can be employed to mitigate server vulnerabilities. Network monitoring can also help to identify potential cybersecurity incidents. Vulnerability management should be implemented and developed according to the IG policy, and audit records should be regularly reviewed.

Exploiting misconfigurations in web application firewalls

It is essential to conduct regular vulnerability scans and perform periodic checks on the system's configurations to identify potential vulnerabilities. Vulnerability scans must be run automatically whenever software packages are updated to ensure proper configuration. Additionally, from an information governance perspective, maintaining audit logs and tracking account changes made to the system can help identify and manage any vulnerabilities. Controls and measures to detect configuration changes are also critical in ensuring the system's security (Neto et al., 2020).

Unauthorized Access to Credentials and Secret Keys

To prevent exploitation, secure vault storage is recommended to maintain Access Key IDs and Secret Keys. Implementing time-dependent role-based access limits administrative accounts to authorized access for a specific duration, reducing the impact of extended attacks. From an IG perspective, proper credential management is crucial, including revocation of access when not in use and logging all user actions. Establishing monitoring, alerting, logging, and alarms for extended external user activity, vendor account activity, and unauthorized activity can help detect and mitigate attacks early on (Neto et al., 2020).

Ability to run commands to list and sync Using Cloud Data Storage

To secure the s3 storage from malicious attacks and information leakage, measures should be taken to protect against data leaks. Additionally, it is advisable to establish and maintain a baseline configuration of IT control systems to incorporate security principles in the organization's file storage system. The Central Bank of

UNDER PEER REVIEW

Nigeria (2015) proposed international standards for information governance in the financial bank industry. These standards are designed to assist banks in developing, implementing, and driving the strategic IT architecture structure and creating a framework for evaluating operations. Ultimately, they will help secure the banks' information and assets.

Figure 6: *Expected Capability Areas and Standards*

	Capability Area		**Standards**
1	Strategic IT Alignment		ITIL/COBIT
2	IT Governance		COBIT/ ISO 38500
3	Architecture & Information Management	Interfaces	ISO 8583 / ISO 20022
		Reporting	TOGAF
		Enterprise Architecture	XBRL
4	Solution Delivery	Applications Development	CMMI-Dev
		Project Management	PMBOK PRINCE2
5	Service Management & Operations	Service Management	ITIL/ ISO 20000
		Data Center	Tier Standards - Tier 942
		HSE	OHSAS 18001
		Business Continuity	BCI GPG/ ISO 22301
6	Workforce & Resource Management		SFIA
7	Information & Technology Security		PCI DSS, ISO 27001/27002

Research Limitations

The findings of this study may not fully reflect the perspectives of many bank executives, and the conclusions may only partially apply to the current situation since the study used secondary data from 2013. Additionally, the sample size was limited to 16 bank executives from 13 banks in Hong Kong, Brazil, and the United States, excluding banks from Europe, Africa, and Australia. To enhance the generalizability and validity of the results, we suggest conducting further empirical tests with a larger sample size that includes banks from different continents.

4. CONCLUSION

Based on the research findings, it has been demonstrated that implementing Information Governance (IG) programs in the banking industry leads to improved profitability. The results of the regression models indicate that the p-value is .05, leading to no rejection of "H*o*" and the acceptance of "Hα." Therefore, with 95% confidence, it can be stated that IG policies does not contribute to mitigating data breaches in the Nigerian banking industry and improving profitability. The study has shown that financial institutions can utilize information governance to mitigate data breaches and increase profits. While data breaches remain a real threat, banks can leverage IG policies to enhance profitability by safeguarding their assets. As a result, Nigerian banks must remain vigilant and address any changes within their business infrastructure to mitigate risks and protect sensitive data using appropriate IG policies and standards.

UNDER PEER REVIEW

References

Aseinov, D., & Karymshakov, K. (2018). Development of the banking system in Kyrgyzstan: An historical review and current challenges. *Sosyoekonomi*, 26(38), 71–86. https://doi.org/10.17233/sosyoekonomi.2018.04.05

Bounagui, Y., Mezrioui, A., & Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: an approach for evaluating and integrating IT management and governance models. *Computer Standards and Interfaces*, 62, pp. 98–118. https://doi.org/10.4018/IJCAC.2016100104

Bruno, M., & Lagasio, V. (2021). An overview of the European policies on ESG in the banking sector. *Sustainability*, 13(22), 12641. https://doi.org/10.3390/su132212641

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Central Bank of Nigeria. (2015). Nigeria banking industry IT standards blueprint. https://www.cbn.gov.ng/itstandards/IT_Standards_Blueprint_Revised%20v3%20104.pdf

Deloitte. (2021). A higher bottom line - the future of financial services. *Deloitte Development LLC Publication*. https://www2.deloitte.com/us/en/pages/financial-services/articles/future-of-financial-services.html

Faria, F. A., & Simpson, G. E. (2013). Bridging the gap between business and IT: An information governance perspective in the banking industry. *Taylor and Francis Group*, 24. eBook ISBN-9780429111358.

Faria, F. A., Macada, A. C. G., & Kumar, K. (2013). Information governance in the Banking industry. *2013 46th Hawaii International Conference on System Sciences*, 4436–4445. https://doi.org/10.1109/HICSS.2013.270

Handa, R. (2018). Does corporate governance affect financial performance: A study of select Indian banks. *Asian Economic and Financial Review*, 8(4), 478–. https://doi.org/10.18488/journal.aefr.2018.84.478.486

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, pp. 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lunardi, G.L., Becker, J.L., Macada, A.C. & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems*, 15(1), 66–81. https://doi.org/10.1016/j.accinf.2013.02.001

Mazumder, M.M., & Hossain, D.M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies, 24.* https://doi.org/10.1108/JAEE-07-2021-0237

Merrick, R., & Ryan, S. (2019). Data privacy governance in the age of GDPR. *Risk Management*, 66(3), 38-40,42-43. https://www.proquest.com/scholarly-journals/data-privacy-governance-age-gdpr/docview/2215472110/se-2

Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the Capital One data breach. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567

Ohiani, A. S. (2021). Technology innovation in the Nigerian banking system: prospects and challenges. Rajagiri Management Journal, 15(1), 2-15. https://doi.org/10.1108/RAMJ-05-2020-0018

Onwujekwe, G., Thomas, M., & Osei-Bryson, K. M. (2019, April). Using robust data governance to mitigate the impact of cybercrime. *In Proceedings of the 2019 3rd International Conference on Information System and Data Mining*, pp.70-79. https://dl.acm.org/doi/pdf/10.1145/3325917.3325923

Pereira, R., Almeida, R. & Silva, M.M. (2014). IT governance patterns in the Portuguese financial industry. *014 47th Hawaii International Conference on System Sciences, 4386–4395*. https://doi.org/10.1109/HICSS.2014.541

Randhawa, T. S. (2019). Incorporating data governance frameworks in the financial industry. *ProQuest Dissertations Publishing*. https://eznvcc.vccs.edu/login?url=https://www.proquest.com/dissertations-theses/incorporating-data-governance-frameworks/docview/2191204944/se-2.

Tanoh, C. N. (2022). Effectiveness of information security governance in the U.S. banking industry: Towards a resilient business perspective. ProQuest Dissertations Publishing. https://eznvcc.vccs.edu/login?url=https://www.proquest.com/dissertations-theses/effectiveness-information-security-governance-u-s/docview/2654124325/se-2.

Uchenna Okoye, L., Ehimare Omankhanlen, A., I. Okoh, J., N. Ezeji, F., & Ibileke, E. (2020).

UNDER PEER REVIEW

Impact of corporate restructuring on the financial performance of commercial banks in Nigeria. *Banks and Bank Systems*, 15(1), 42–50. https://doi.org/10.21511/bbs.15(1).2020.05

Wang, P., D'Cruze, H., & Wood, D. (2019). ECONOMIC costs and impacts of business data breaches. *Issues in Information Systems*, 20 (2). https://pdfs.semanticscholar.org/c104/5c170e6f7cbd31423354dbf93eef4eb1dd1a.pdf

Wallarm website. (n.d.). https://www.wallarm.com/what/waf-meaning

Warren, D. (2021). Storing, Retrieving & Implementing Objects using AWS S3. https://aws.plainenglish.io/storing-retrieving-implementing-objects-using-aws-s3-e2b206e98623

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21 (1). https://doi.org/10.1093/rof/rfw074

UNDER PEER REVIEW