International Journal of Financial and Business Studies (IJFABS)
https://ijfabs.org/journals/
ISSN: Online-2811-1664; Print-2811-1656

THE IMPACT OF THE JUDICIARY ON CYBERSECURITY CRIMES IN BUSINESS AND FINANCIAL SECTORS: A CRITICAL ANALYSIS.

Onwuka Tochi Chukwudi Esq

Department Legal Studies, School of General Studies,

Federal Polytechnic, Oko, Anambra State, Nigeria

Email: tochi.onwuka@federalpolyoko.edu.ng or debelovedtochi@gmail.com

08033880767, 08139908403

Abstract: The increasing occurrence of cybercrimes poses a critical and consequential challenge to the business and financial sectors, hence necessitating judicial responses to address these threats. This paper explores the impact of the judiciary on cyber security crime through the lens of legal framework, enforcement mechanism, and case law. It analyses how judicial decision structure cyber security policies and practices within business and financial sectors, influencing compliance standards and risk management techniques. The research identifies trends in judicial interpretation of cybercrimes legislation, outlining the role of judiciary in setting legal precedent and ensuring accountability Also, the research discussed the validity of judicial system in deterring cybercriminal activity, advocating the importance of cooperation amongst the cyber security collaborators and legal institution. The findings highlight the need for a flexible legal framework comprising a specialized knowledge for judiciary, prompt response to cybersecurity cases, interpretation and application of current cybersecurity laws and regulation etc that moves in line with technological advancements, aiming to enhance the adaptation of the business and financial sectors against cyber threats. This research contributes to a clearer understanding of the judiciary's influence in shaping cyber security environment, offering recommendations for policymakers, legal practitioners and business to enhance legal framework for cybercrime.
Keywords: Cyber security crimes, Impacts of Judiciary on cybercrime, Cyber security crime on business and financial sectors.

Introduction

The judiciary's impact on cybersecurity crime in business and financial sectors is profound. It not only assists in the prosecution of cybercriminals, but also empowers business and financial sector to increase their cybersecurity measures, thereby promoting a safer and more resilient economy. They play a crucial role in shaping the legal landscape of cybercrime. Through their decisions, judges interpret and apply laws related to cybercrimes, influencing the development of jurisprudence in the area. In this computer age, businesses and financial institutions faced exceptional and remarkable challenges posed by cybercrime, requiring strong measures for protection and accountability. The judiciary plays a pivotal role in shaping the legal framework that governs cybersecurity, addressing both compliance and enforcement measures around these sectors. Through the creation of laws, Interpretation of existing regulations, and adjudication of related cases, the judiciary does not only provide a landscape for obviating cybercrime but also ensures that businesses are held accountable for breaches and lapses in security. The Judiciary is oblige to make and interprets laws that will help to curb cybercrime in business and financial sectors.

The impact of the judiciary on cybercrimes includes various aspects of development of legal standards for data protection, the clarification of liability in cases of data breaches, and the enforcement of penalties for cybercrimes. The judiciary influences how business and financial sectors implement safeguards against cyber threats by giving interpretations on various statutes related to cybersecurity; hence ensuring that these sectors adopt proactive strategies to protect sensitive information and maintain customers' trust.

However, cybersecurity laws cannot exist without judiciary. The judicial decisions contribute to the evolution of cybersecurity law, which addresses threats and challenges as technologies emerges. In this era where criminals utilize sophisticated techniques to exploit susceptibilities, the responses of the judiciary in shaping policy and legislation, helps to encourage innovation in cybersecurity practices and foster a safer digital ecosystem.

Statement of the Problem

A number of factors like rapid advancement of technology, high rate of unemployment, quest for quick wealth, and the increasing reliance on digital platforms for business and financial operations have led to a significant rise in cybersecurity crimes. Despite the continuous and persistence fight in safeguarding sensitive data and financial transactions, most businesses still faced challenges in mitigating cyber threats. However, the role of the Judiciary in shaping the legal framework sounding cybersecurity cannot be undermined, yet, its impact on curbing cybercrime in the business and financial sectors remains inadequately explored.

The researcher seeks to analyze the effectiveness of current judicial mechanisms and laws in combating the complexities of cybersecurity. Also to assess whether the existing legal framework is adaptable to the evolving nature of cybercrimes and whether judicial responses adequately prevent malicious activities. Besides, this is achieved by examining how judicial decisions influence the development of cybersecurity policies, the enforcement of laws against cybercriminals, and the protection of business and financial sectors from cyber threats.

By investigating the interaction between the judiciary and cybersecurity crimes in business and financial sector, this research aims to highlights areas for further study in legal responses, propose recommendation for strengthening judicial effectiveness, and contribute to the broader discourse on enhancing cybersecurity measures in these critical sectors.

Conceptual Framework

The Concept of Cybersecurity Crimes

Cybersecurity crimes, often called cybercrimes, e-crime or hi-tech, are illegal activities conducted via the internet or involving computer technology, aimed at achieving various malicious objectives like data theft, fraud, or disruption of services. These crimes targets individuals, organizations, or government entities and exploit vulnerabilities in systems, networks, and devices. A computer crime encompasses criminal activities which can aptly be categorized by its unique typology of computer related crime, comprising conventional crimes in which computers are instrumental to the offence.[1] The first published report of cybercrime occurred on the mainframe computer in the 1960s[i]. These cybercrimes can come in form of malware attacks, phishing,

Denial-of-service (DoS) attack, Social Engineering, and Data Breaches etc. They have common characteristics like:

1) Anonymity: it can mask its identities, making detection and prosecution challenging.

2) Global Reach: The internet allows cybercriminals to operate across jurisdiction, complicating the effort of laws enforcement.

3) Rapid Evolution: Cyber threats evolve quickly as criminal adapt to technological advancement and emerging trends.

4) Low cost and high reward: The level of high reward from cybercrimes when compare with the low operational costs attract more people into criminal activities. etc.

The Widespread Impact of Cybersecurity Crimes

As cybersecurity threats continued to evolve, they are not without a significant impact, aimed to exploit vulnerabilities. Cybersecurity crimes have both direct cost and indirect cost on the economy like, reputational damage and loss of consumer trust. Cyber bullying and identity theft can have severe psychological effects on individuals, while broader societal impacts include erosion of trust in digital communications. Lastly, cybercrimes can be a great threat to national infrastructure, critical services, and governmental operations, hence raising concerns over state security.

Cyber Security Crime on Business and Financial Sectors

Globally, a cybersecurity crime poses a significant threat to businesses and financial institutions. It has jeopardized sensitive data, financial resources, and consumer trust. Since most organizations are increasingly reliant on digital technologies, the risk of cyberattacks evolves and inevitable, there-by creating a concern for robust cybersecurity measures. Most business and financial sectors records significant financial losses due to cyber theft, ransom payments, and recovery costs. The average cost of data breach runs in millions of dollars, including immediate losses and long-term reputational damage. The reputational damage can come in the form of dilapidation of customer's trust and brand integrity. Customers on this note may hesitate to engage with businesses, leading to decreased sales and customer loyalty. Additionally, businesses and financial institutions often face stringent regulatory requirements regarding data protection, and compliance most cases attract hefty fines and legal actions. A lot of business operations are disrupted by cyberattack, affecting service delivery and productivity, hence leading to further financial implications and customer dissatisfaction.

Impacts of Judiciary on Cybercrime

As digital technology spread speedily, so do the methods used by the cybercriminals, necessitating a responsive and adaptive legal landscape. On their wisdom Emmanuel O, and others said that as the technology evolves, so too do the methods used by cybercriminals, and outdated legal frameworks are often inadequate to handle these

new challenges.[2] The judiciary plays a significant role in shaping the legal framework through the interpretation and enforcement of laws related to cybersecurity. Through the adjudication of cases of cybercrime, the judiciary not only imposes penalties but also influences legislative developments and established precedents that guide businesses and financial institutions in their security practices. This section explores the impact of the judiciary on cybercrime as buttress below:

1) Judicial Interpretation and Application of cybercrime laws

The judicial interpretation and application of cybercrime laws are critical in determining the scope and effectiveness of these laws. One thing is to interpret the laws and the other is to apply these laws in a way it will protect both individuals and public sectors from cyber threats. Judges must balance the need to protect individuals and organizations from cyber threats with the need to ensure that laws are not overly broad or restrictive. In the case of United States v. Lori Drew[3] the United States District court considered the application of the Computer Fraud and Abuse Act (FAA)[4] to online harassment. The court's decision highlighted the challenges of applying traditional laws to emerging forms of cybercrime. In the same vein the court highlighted the complexities of applying the CFAA to online activities in the case of United States v. Nosal[5]. However, the court's decision on the case of R v. Mcnulty[6] emphasized the importance of protecting individual privacy in the digital age.

2) Judicial Activism and Cybercrime

The judiciary plays an active role in shaping the laws on cybercrimes through judicial activism. Judges can help to ensure that the legal system remains effective in addressing cybercrime, by interpreting laws in a way that is responsive to emerging cyber threats. In his wisdom Justice K.K Usha in the case of Shreya Singhal v. Union of India[7] struck down section 66A of the Information Technology Act[8] and demonstrated the importance of judicial oversight in ensuring that cybercrime laws are constitutional and do not unduly restrict individual rights.

3) Legal Framework Governing Cybercrime

The legal framework governing cybercrime is derived from a mix of statutory laws, common law principles and international treaties. The computer Fraud and Abuse Act (CFAA)[9] in the United States serves as a primary

statute aimed at combating cybercrime by prohibition unauthorized access to computer systems. Other similar frameworks include: the EU's General Data Protection Regulation (GDPR)[10] and the UK's Computer Misuse Act 1990[11], which impose stringent requirements on organizations to secure personal data. The interpretations given to these laws by the judiciary plays a significant role in determining their applicability and scope. In the case of United States v. Morris[12] for example, the court defined "exceeding authorized access" under the CFAA. The case involved a computer virus created by Robert Tappan Morris that impacted thousands of systems. The court's ruling clarified or defines what constitutes unauthorized access, setting a precedent for future cases involving similar offenses.

4) Judicial Interpretation and Precedent

As earlier noted, judiciary's interpretation of cybersecurity laws critically shapes the legal meaning of statutes. In re Sony Gaming Networks and Customer Data Security Breach litigation[13], the court dismissed claims against Sony on the ground that the company did not owe a specific duty to protect users from unknown harms. The case addresses the challenge of establishing a legal duty in cybersecurity issues and set a precedent for similar cases where organizations face scrutiny for data breaches.

5) Impact on Business Practices

The decisions of the judiciary have profound implications for business practices regarding cybersecurity. Companies are obligated to embrace preventive measures and develop comprehensive cybersecurity policies to protect sensitive data, hence mitigating legal risk. The court in the case of FTC v. wyndham worldwide Corp. affirmed the Federal trade Commission's (FTC)[14] authority to regulate cybersecurity practices under the unfair or deceptive acts and practices (UDAP) standard. It also held that inadequate cybersecurity measure could qualify or seen as deceptive acts, hence encouraging companies to increase their cybersecurity protocols or dance the music of legal repercussions.

Additionally, the judiciary has influenced corporate governance regarding data protection. The court demonstrated how it can enforce compliance with data protection practices in the case of Facebook, Inc. v. Alterations to user data handling.[15] The outcome of the case illustrated that companies must prioritize user data protection or risk significant penalties, further embedding cybersecurity into the corporate governance framework.

6) Judicial Role in International Collaboration and Jurisprudence

Looking at the global nature of the internet, it necessitates international cooperation in combating cybercrime, and the judiciary plays a significant role in this collaboration. International treaties like the Council of Europe's Budapest convention on cybercrime[16] emphasize the need for effective cross-border legal cooperation to address cyber threats. Judicial authorities are regularly called upon to interpret these treaties within their legal systems, hence increasing international cooperation. The case of United States v. Microsoft Corp[17] is a good case that can be used to

Methodology

Research Design

This is the specification of methods and procedures for acquiring the information needed for the research. Ex-post facto research design was used. This study is historical in nature and it covers ten years annual report of companies under study starting from 2011 to 2020. This study was done in Nigeria and it covers a | year period from 2011 to-2020.

Population of the study

The population of this study was made up of twenty (20) giant listed companies in Nigeria. They include:

1. Dangote Cement Plc
2. Zenith Bank Plc
3. Nigerian Breweries Plc
4. First Bank Plc
5. United Bank of Africa
6. First City Monument Bank
7. Unilever Nigeria Plc
8. Cadbury Nigeria Plc
9. Stanbic IBTC
10. Access Bank Plc
11. Union Bank of Nigeria Plc

[17] (2018) 138 S. Ct. 1202

12. Guinness Nigeria

13 Flour Mills of Nigeria Plc

14. Guaranty Trust Bank Plc

15. Lafarage Cement WAPCO Nigeria Plc

16. Total Nigeria Plc

17. Unilever Nigeria Plc

18. PZ Cussons Nigeria Plc United Bank of Africa

19. UACN

20. Nestle Nigeria Plc

For the purpose of this study, data were obtained from the company's websites and published annual report of the companies under study. The technique used in analyzing the formulated hypotheses for the study is the multiple regression technique done with the aid of SPSS (Statistical Package for Social Sciences) version 23.0. The study also used GRI 3.1 to analyze economic, environmental and social performance disclosure index. In doing this, content analysis was used to extract data from Global Reporting Guideline.

Sample and sampling Techniques

Due to the fact that our population is not large we therefore adopt the whole companies as our sample size.

Data Analysis and Results

Recommendations

From the study, the following recommendations are made to enhance sustainability reporting.

1. Sustainability reporting should be encouraged and a regulatory body set up to see that company's include sustainability report in their annual report as the study has shown there is a significant effect of sustainability reporting on company's performance.

2. Companies should be encouraged to disclose economic performance as this may increase their performance in the long run.

3. Since companies have not been complying fully to international best practices, there should be mandatory localized environmental reporting framework in line with international best practices on issue of sustainability reporting.

4. Companies should maintain a good relationship with their employees, suppliers, local communities and others concerned and report this appropriately in their annual report as this has an effect on their performance.

Contribution to Knowledge

To the best of our knowledge this study has contributed to the body of existing literature by looking into the effect each of the component of sustainability: economic, environmental and social has on company's performance. The study also contributed to knowledge by finding out that economic performance disclosures has no significant effect on return on asset.

Suggestions for Further Study

Since we have different financial performance indicators, the researcher suggests that further studies should be carried out using other indicators such as return on equity, or a market performance indicator like market share. Further research can be carried on least performing companies covering same number of years or a broader number of years.

Conclusion

In this study, effort has been made to examine the effect of sustainability reporting on company's performance. The study has four specific objectives: to determine the effect economic, environmental and social performance disclosures have on company's performance. The study made use of secondary data. The study found that economic performance disclosure and environmental performance disclosure has no significant effect on company's performance while social performance disclosure has a significant effect on company's performance. Mandatory localized reporting framework in line with international best practices should be put in place to encourage sustainability reporting.

References

Adams, M., Thornton, B. and Sepehri, M. (2013). The impact of the pursuit of sustainability on the financial performance of the form. Journal of Sustainability and Green Business, 5 (1), 213-230. Retrieved from

' http://www.aa.bn_.CQrn/maniiscript/107Q6.pdf

Andrea, K. K. (2012). Performance indicators in CSR and sustainability reports in Hungary. Applied Studies in Agric business and Commerce, 42(8), 62-75, doi: 10.1901/abstract/2012/3-4/20

Annisa, H. N. and Wiwin, B. (2012). The impact of sustainability reporting on company performance. Journal of Economics, Business and Accountability Ventura, 15(2), 257-272, Accreditation No. 110/DIKTI/kep/2009

Borial, O. (2013). Sustainability reports as simularia? A counter-account of Aand A+ GRI reports. Accounting, Auditing and Accountability Journal, 26, 1036-1071

Brundtland, G. H. (1987). Our common future. United nations world commission on environment and development (Brundtland commission). Oxford: Oxford university press. Bsigroup; How sustainability standards can drive business performance, bsigroup.com

Carrot, M. and Sticks, C. (2013), "Promoting transparency and sustainability". Retrieved from www.gliAalreporting.o.rg/Fcsi)i.ircesl,!brary

Cho, C. G. and Pattern, D. M. (2007). The role of environmental disclosures as tools of legitimacy: A research more. Accounting, Organization and Society Journal, 32 (7-8), 639-647. http://dx.doi. org/10.1016/j.aos.2006.09.009

Choi, Frederick, D. S. & Gary, K. M. (2008). International accounting. 6th edition, New Jersey: Pearson

Prentice Hall.

Deegan, C. (2000). Financial Accounting Theory Irwin McGraw-Hill, Sydney.

Deegan, C. (2002). The legitimizing effect of social and environmental disclosures: A theoretical foundation. Accounting, Auditing and Accountability Journal, 15(3), 282-311. http://dx.doi. org/10.1 108/09513570210435852

Ernest, M. and Young, O. (2009). Non- financial reporting. Retrieved Sept. 15, 2016from http://:www. ey.com/publication/vwLU Asset/Non-

financial_reporting/$FILE/Climate%20Change_Non%20 fnancial%2 Oreporting.pdf Forbes Africa (2012). Twenty fve top performing West African Companies. Retrieved from http://:www.cp-africa.com/tag/the-top-listed-west- african-companies-by-forbes

Francisco, S. and Zahir, D. (2014). Transparency, a new strategy to communication- : - "sustainability performance .hit;1:'

Freeman, J. M. (2009). Optimal policies for playing variable wager HILO. Journal of Operational Research Society, 60 (1), 79-83, DOI: 10.1057/plagrave.j.ors

2602520.

Freeman, R. E., Wicks, A. C. &Parmar, B. (2004). Stakeholder theory and the corporate objective revisited. Organization science, 15(3), 364-369.

Gentry, C. R. (2007). Full disclosure: Shareholders urge companies to reveal sustainability practices, chain stone age, 83(10), 177-1

Gray, R., Kouhy, R. and Lavers, S. (1996). Corporate social and environmental reporting: A review of the literature and a longitudinal study of UK disclosure. Accounting, Auditing and Accountability Journal, 8(2), 47-77. http://dx.doi.org/10.1108/09513579510146996

GRI (2011) G3.1 Sustainability reporting guidelines, global reporting initiatives. http://www. globalreporting.org/resourcelibrary/G3.1 -guidelines- inc-technical-protocol .pdf

Herdberg, C. I. and Mamborg, V. F. (2003). The global reporting initiative and corporate sustainability reporting in Swedish companies. Social responsibility and environmental management, 10, 153-164.

Hong, Y. C., Fabio, G. &Thiago, G. T. (2014). Scoring sustainability reports using GRI indicators: A study based on USE and FTSE4 good price indexes. Journal of management research, 6(3), doi:10.5296/jmr.v613.5333 ' ,

Isa, A. M. (2014). Sustainability reporting among Nigeria food and beverage firms. International Journal of Agriculture and Economic Development, 2(1), 1-9. KPMG (2008). KPMG international survey of corporate responsibility reporting retrieved from www.kpmg.com/global/ensured and insights/ articles/publications/pages/sustainability- reporting-2008.aspx

KPMG (2011). Corporate sustainability: A progress report. http://www.kpmg.com/global/en/issues and insights/articles

publications/documents/corporate sustainability-v2.pdf

Lopez, M. V., Garcia, A. & Rodriguez, L. (2007). Sustainable development and corporate performance: A study based on Dow Jones sustainability index.

Journal of Business Ethics, 75, 285- 300. http://dx.doi.org/1 0.1007/s 10551 -

006-8253-8

Lorenzo, G. (2009). A generalized approach to portfolio organization: improving performance by constraining portfolio morns Management science 55 (5), 798-812.

O'Donovan, G. (2002). Environmental disclosures in the annual report: Extending the applicability and predictive power of legitimacy theory. Accounting, Auditing and Accountability Journal, 15(3), 344-371. http://dx.doi.0rg//10.1108/09513570210435870

Okafor, T. G. (2018). Environmental costs accounting and reporting on firm financial performance: A survey of quoted Nigerian Oil Companies. International Journal of Finance and Accounting, 7(1): 1-6. d

10.5923/j.ijfa.20180701.01.

Onyinyechi, O. C., &Ihendinihu, J. U. (2016). Impact of environmental

corporate social responsibility accounting on organizational financial: performance: Evidence from selected listed firms in Nigerian Stjbck" Exchange. Journal of Emerging Trends in Economics arid Management Sciences, 7(5), 291-306. " -;:;^

Orazalin, N. (2020). Do board sustainability committees contribute to corporate environmental and social performance? The mediating role of corporate social responsibility strategy. Business Strategy and the Environment, 29, 140-153. https://doi.org/10.1002/bse. 2354

Parliament of Austrialia (2010). Sustainability reporting practices, performances and potential. A research project commissioned by CPAustrialia. Retrieved http://:www.aph.gov.au?About_Parliament /Paeliamentary_Departments/Parliamentary_Library/pubs/rp/ BudgetReview201112/sustainability

Pieter, B., Merwe, O. &Panagiotis, A. (2011). An investigation of the economic performance of sustainability reporting companies versus non- reporting companies: A South African perspective. Journal of Social Science, 29(2), 151-158.

Post, C., Rahman, N., and McQuillen, C. (2015). From board composition tocorporate

Priyanka, A. (2013). Impact of sustainability performance of company on it'sfnancial performance: A study of listed Indian companies. Global Journal Inc.,13, 2249-4588.

Rahardjo, H., Idrus, M. A., Djumilah, H., &Siti, A. (2013). Factors that determine the success of corporate sustainability management. Journal of Management Research, 5(2). http://dx.doi. org/10.5296/jmr.v512.2993

Rao, K., Tilt, C., & Lester, L. (2012). Corporate governance and environmental reporting: An Australian study. Corporate Governance: The international journal of Business in Society, 12(2), 143-163. https://doi.org/10.1108/14720701211214052

Rossi, A. &Tarquinio, L. (2017). An analysis of sustainability report assurance statements. Evidence from Italian Listed Companies. Managerial Auditing Journal. 32. 10.1108 /MAJ-07-2016-1408.

Rupley, K., Brown, D., & Marshall, R. (2012). Governance, media and the quality of environmental disclosure. Journal of Accounting and Public Policy, 31(6),610640