

Corporate Governance in Nigeria Amid Digital Transformation

Corporate Governance & Regulatory Compliance Insights



2 Introduction

**3 Emerging Technologies and their
Impact of Corporate Governance**

**8 Cybersecurity Threats and Board
Responsibilities**

**9 Adopting a Proactive Cyber
Governance Approach**

11 Conclusion



1. Introduction

Digital transformation signals a fast-moving shift in how innovation, technology, and data are used in businesses and for corporates, it has become a necessity for economic success and a requirement that touches every sphere of the business.

It therefore goes without saying that technology has become integral to modern business operations, and its influence is only expected to grow. The integration of digital technology into all areas of a business is fundamentally changing how organisations operate and delivers value to stakeholders. This change is also affecting governance processes, as companies look for ways to employ technology in improving their business models, operational efficiency, decision-making processes and more.

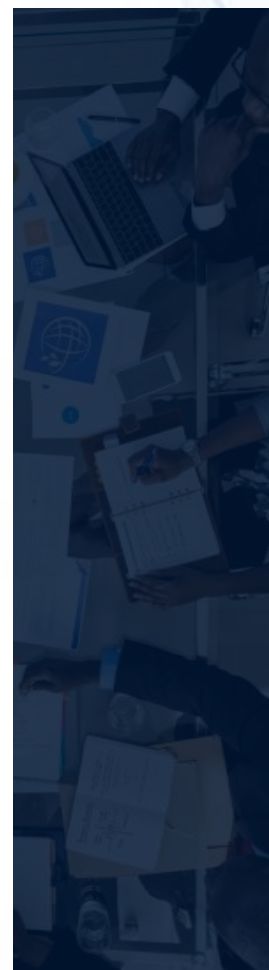
For board and senior management teams, the pertinent question is now how to navigate the changes that digital innovations pose to a company's daily operations. Navigating these innovations are necessary not only for the organisation's daily operations but also for how board of directors fulfil their governance roles. It has thus become essential for boards to adopt a flexible, technology-driven approach to address the rapid changes brought about by technological innovation.

Digital innovations such as blockchain, big data analytics, artificial intelligence and cybersecurity systems have had a positive impact on decision-making, risk management, and compliance. While these innovations present remarkable opportunities for growth, efficiency, and value creation, they also bring new challenges, including cybersecurity threats and ethical concerns.¹

Discussions have erupted amongst company leaders and regulators regarding emerging technological and effective transitions from reactive governance models to proactive frameworks that anticipate and mitigate possible risks. This also highlights the need for regulators to promote an enabling environment for the utilisation and growth of emerging technologies and to establish robust policies and frameworks incorporating elements of digital oversight, ethical artificial intelligence deployment, and proactive cybersecurity risk management.

This paper explores how digital innovations impact corporate governance. It emphasises the necessity for governance models that proactively integrate technology rather than reactively.

¹ Z. Korachi and B. Bounabat, *Integrated Methodological Framework for Digital Transformation Strategy Building (IMFDS)*, International Journal of Advanced Computer Science and Applications, vol. 10, no. 12, 2019, DOI: 10.14569/ijacsa.2019.0101234.[4] Z. Korachi and B. Bounabat, *General Approach for Formulating a Digital Transformation Strategy*, Journal of Computer Science, vol. 16, no. 4, pp. 493-507, 2020, DOI: 10.3844/jcssp.2020.493.507





2. Emerging Technologies and their Impact of Corporate Governance

Emerging technologies ushered in by the Fourth Industrial Revolution have remarkably transformed several industries and restructured traditional business models.² Corporate governance has also witnessed significant transformation, with governance structures revised to adapt to the current technological realities. Therefore, there is a need to re-evaluate traditional corporate governance practices in light of modern digitalisation.³

So far, these technologies have offered significant benefits to corporate governance.⁴ It has highlighted the necessity for flexibility of corporate governance structures, enabling companies to realign their strategies in response to technological innovations. In the same vein, they have also highlighted the need for digital literacy at the board level to provide informed oversight on digital transformation, AI ethics and even cybersecurity. Moreover, technology will impact the corporate governance aspects of decision-making, transparency, accountability, compliance, risk management, data processing, and stakeholder engagement, among others.

- a. **Artificial Intelligence (AI):** AI is not a new concept; it is believed that John McCarthy and Myron Minsky realised the first usage of artificial intelligence in the mid-1950s.⁵ There is no general definition of AI, as its definition has changed several times since its inception. However, AI is widely accepted as a system that imitates human behaviour.⁶ Although there are numerous definitions of AI, it could be described in four categories: “systems could think as humans do”, “systems could act as humans do”, “systems could think in a rational way”, and “systems could act in a rational way”.⁷

AI is poised to significantly impact corporate governance by enhancing decision-making, automating processes, and improving risk management. Its ability to analyse vast quantities of data at remarkable speeds allows AI to identify patterns and trends that might otherwise go unnoticed. This capability enables boards and management teams to make more informed strategic

-
- 2 What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?,(2022) McKinsey and Company, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir>
 - 3 O. Ojo., (2024), *Corporate Governance in the Digital Era: Trends and Best Practices* - trustedadvisorslaw.com. <https://trustedadvisorslaw.com/corporate-governance-in-the-digital-era-trends-and-best-practices/>
 - 4 Tong Wu, (2024), *Exploring of the Integration of Emerging Technologies and Corporate Governance*, Nottingham University Business School, University of Nottingham Ningbo, Ningbo, Zhejiang, 315199, China, Proceedings of the 2nd International Conference on Management Research and Economic Development DOI: 10.54254/2754-1169/87/20241021
 - 5 John Armour and Horst Eidenmüller, *Self-Driving Corporations?* (2019), Harvard Business Law Review/44; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442447, p. 92,
 - 6 Joost N. Kok, Egbert J. W. Boers, Walter A. Kusters, and Peter van der Putten, “Artificial Intelligence: Definition, Trends Techniques, and Cases”(2009) , available at @Encyclopedia of Life Support Systems (EOLSS), <https://www.eolss.net/ebooklib/bookinfo/artificial-intelligence.aspx> 2.
 - 7 Joost N. Kok, Egbert J. W. Boers, Walter A. Kusters, and Peter van der Putten (Ibid)



decisions. In addition, AI-driven compliance solutions can automate regulatory compliance monitoring, thereby minimising human errors. These solutions offer real-time auditing and reporting, encouraging greater accuracy, increased transparency, and enhanced accountability in governance processes.

- b. **Blockchain:** Blockchain technology is defined as a decentralised and distributed ledger that records and validates the authenticity of digital assets, ensuring that registered transactions cannot be altered retroactively.⁸ Blockchain operates as a peer-to-peer network where every node or member has access to the entire database and its history.⁹ Dates and information recorded on the decentralised ledger are not controlled by a single individual, allowing records of transactions inputted by different people to be independently verified without the need for an intermediary.¹⁰ This decentralisation is a key feature that makes blockchain secure and transparent.

The structure of blockchain is such that it is immutable. Once a transaction is recorded, it cannot be altered¹¹ or modified without changing or modifying all successive blocks.¹²

In Nigeria, the adoption of blockchain technology is being explored across various sectors. The National Blockchain Adoption Strategy, developed by the National Information Technology Development Agency (NITDA), outlines the roadmap for integrating blockchain into government operations to enhance transparency, efficiency, and security. The objective of the strategy is also to identify and utilise the opportunities provided by Blockchain technologies to strengthen the country's security in cyberspace.

Blockchain technology has the potential to enhance the transparency, accountability, and efficiency that define corporate governance mechanisms. By leveraging blockchain's secure and transparent features in recording and authenticating decisions and transactions, core governance principles, accountability, transparency, and protection of shareholders, are reinforced considerably. The decentralised and immutable feature of blockchain ensures the permanence of all the recorded data, making the likelihood of fraudulent activity minimal. This ultimately enhances an unaltered audit trail that can be examined by shareholders, auditors, and even regulatory agencies, thereby promoting accountability and transparency.

8 Definition as provided by the National Blockchain Adoption Strategy

9 Blockchain Technology: Revolutionizing Data Integrity and Security - Lukmaan IAS Current Affairs. <https://blog.lukmaanias.com/2024/12/07/blockchain-technology-revolutionizing-data-integrity-and-security/>

10 Stock Market News 'Blockchain Facts: What Is It, How It Works – Stockmarkets'. <https://stockmarkets.co.in/terms/blockchain-facts-what-is-it-how-it-works-and-how-it-can-be-used>

11 Definition as provided by the National Blockchain Adoption Strategy

12 Grupo-Mio, 'Understanding Blockchain: The Future of Trust and Transparency' – Grupo-Mio. <https://grupo-mio.com/understanding-blockchain-the-future-of-trust-and-transparency/>



Additionally, blockchain technology can revolutionise shareholder voting systems by introducing smart contracts that automate voting processes. This use case ensures accurate vote tallying, secure records, and protection from manipulation or fraud. In addition, blockchain can enhance compliance and reporting processes by providing real-time access to financial and operational data. This improved accessibility of information enables organisations to meet regulatory requirements with increased efficiency, thereby reducing the risk of non-compliance.

- c. **Big Data Analytics:** Big Data Analytics refers to the examination of large and varied data sets, or big data, to reveal hidden patterns, unknown correlations, market trends, customer preferences, and other valuable information that can help organisations make informed business decisions.¹³ The concept of big data analytics is rooted in the ability to analyse data sets that are too large or complex for traditional data-processing application software to handle.

Big data analytics is increasingly recognised as essential for Nigeria's economic expansion and advancement. The Nigeria Data Protection Act of 2023, which governs the management of personal data, is an important legislation that also oversees the use of big data analytics in Nigeria. This Act ensures data controllers and processors adhere to data protection guidelines, including obtaining consent from data subjects, ensuring data accuracy, and implementing security measures to protect personal information.

Big Data Analysis has the potential of enhancing corporate governance by streamlining the processes for identifying and assessing performance while at the same time aiding the early detection of potential risks and threats by analysing trends and patterns in financial, operational, and compliance data. Through the use of data analysis, companies can predict potential threats before a crisis, thus enabling them to adopt appropriate mitigation measures. In addition, Big Data Analytics can detect fraud by analysing transaction data and identifying anomalies, which is particularly valuable in industries like finance and insurance, where fraud can result in significant financial losses.

Big Data Analytics can enhance decision-making by evaluating the performance of management and board through key performance indicators and other relevant data. This insight aids in executive compensation, promotions, and succession planning decisions. Lastly, analytics tools can monitor compliance by analysing data related to financial reporting, insider

13 Leveraging Big Data Analytics for Competitive Advantage in Singapore - IT Solutions in Singapore.
<https://vgoshinfo.sg/leveraging-big-data-analytics-for-competitive-advantage-in-singapore/>



trading, and other regulatory requirements. This helps organisations minimise the risk of legal penalties and protect their reputation.

- d. **Cloud Computing:** The Nigeria Cloud Computing Policy, (NCCP) 2019, defines Cloud computing as a model for ubiquitous, convenient, on-demand, and real time network access pool of configurable and rapidly provisioned computing resources, including networks, servers, storage, applications and services, among others. Simply speaking, cloud computing is a transformative technology that provides on-demand access to computing resources over the internet, including data storage, servers, databases, and software, instead of relying on a hard drive or a local server.¹⁴ It enables organisations to scale their IT resources according to demand, optimising costs and enhancing operational efficiency.

The NCCP 2019 provides a comprehensive framework for the adoption of cloud computing in both the public and private sectors. The policy was issued by the National Information Technology Development Agency (NITDA) and is applicable to all Federal Public Institutions and corporations owned by the Federal Government. Additionally, the Cybercrimes (Prohibition, Prevention, Etc.) Act plays a crucial role in ensuring the security and protection of data processed through cloud computing. This Act provides a legal framework for the prevention and prosecution of cybercrimes, which is essential for maintaining the integrity of cloud-based systems.

Cloud computing technology presents the potential to fundamentally transform corporate governance, particularly in data storage, management, and accessibility. Leveraging cloud computing will enable organisations to intentionally or unintentionally practice data redundancy, facilitate disaster recovery, and maintain regulatory compliance.¹⁵ Adopting cloud computing gives room for a flexible operating expenditure system and reduces capital investments in IT infrastructure.

Additionally, by offering real-time access to data and analytics, cloud computing promotes transparency by facilitating better accountability and well-informed decision-making. Additionally, cloud platforms foster collaboration by offering shared resources and tools that streamline communication and enhance governance processes. This improved connectivity encourages innovation and strengthens corporate oversight.

14 S. Sunjara., I. Smalley., (2025), 'What is cloud computing?' <https://www.ibm.com/think/topics/cloud-computing>

15 Gurbir Singh (2022), 'Redundancy in Cloud Computing: Key Benefits and Considerations', Synopsys, <https://www.synopsys.com/blogs/chip-design/benefits-of-redundancy-in-cloud-computing.html>



- e. **The Internet of Things (IoT):** The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.¹⁶ IoT devices are also known as smart objects and can be simple smart home devices, smartwatches, RFID-enabled clothing, or complex like industrial machinery and transportation systems. These digital platforms have the ability to analyse the data and assist humans in automatic decision-making and action-taking.¹⁷

In simple terms, internet of things refers to the network of physical objects or “things” embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet.¹⁸ By facilitating real-time data collection and analysis, IoT has the potential to revolutionise several industries and enhance productivity.¹⁹

In Nigeria, the regulatory framework for IoT is still evolving. Nevertheless, the Nigeria Data Protection Act, 2023 plays a vital role in ensuring that personal data collected through IoT devices is processed in accordance with data protection principles. Furthermore, the National Information Technology Development Agency (NITDA) is responsible for the promotion and regulation of the use of information technology in Nigeria, including that of IoT.

The use of the Internet of Things (IoT) in corporate governance structures offers wide-ranging opportunities for increasing transparency, accountability, and efficiency of operations. IoT devices collect real-time data, allowing board members to make informed strategic decisions. Additionally, the IoT enables monitoring of environmental considerations, health, and workplace safety as well as adherence to a range of compliance regulations. This provision ensures that the board members are supplied with accurate and timely information, thus improving the standard of decision-making as well as accountability.

Moreover, IoT enables greater transparency through provision of instant access to important information and analysis, enhancing visibility across company operations. Through IoT use in governance frameworks, Nigerian companies will contribute to sustainable development, improve risk oversight, and maintain stakeholder confidence.

16 IBM, (2023) 'What is the Internet of Things (IoT)?', <https://www.ibm.com/think/topics/internet-of-things>

17 The Nigeria Cloud Computing Policy, (NCCP) 2019

18 H. Pinter (2024), 'The Internet of Things (IoT): A Comprehensive Overview'. <https://ringmovil.com/iot/>

19 Moin, Armin, and João Ferreira. "Model-Driven Engineering Techniques and Tools for Machine Learning-Enabled IoT Applications: A Scoping Review." *Sensors*, vol. 23, no. 3, 2023, p. 1458.



Despite the positive impact technology may have on corporate governance, there are still some shortcomings that must be considered when integrating technology into governance. With technology comes concerns about algorithmic bias, the opacity of automated decision-making, technological complexity, a lack of digital literacy data, privacy issues, the risk of vendor lock-in, inadequate data infrastructure, regulatory uncertainty, and cybersecurity threats.

3. Cybersecurity Threats and Board Responsibilities

Cybersecurity threats are one of the most pressing challenges of deploying technology in corporate governance. Cyberattacks have become more sophisticated and frequent, targeting critical infrastructure, intellectual property, and customer data. For instance, ransomware attacks have escalated in scale and impact, with attackers demanding exorbitant sums to release encrypted data.

Cybersecurity is now a fundamental governance duty rather than just a technical consideration for boards. The financial, legal, and reputational repercussions of a cyberattack underscore the need for robust oversight and proactive risk management. A notable example is the 2017 Equifax data breach, which exposed the personal information of 147 million people.²⁰ In addition to the billions of dollars in fines and settlements the company had to deal with, the incident highlighted the importance of board-level monitoring and ensuring cybersecurity.

The board's responsibility to ensure adequate measures are put in place to prevent and respond to cybersecurity threats cannot be overemphasised. Various regulations have provided a framework to ensure that the board's internal controls and risk management duties are constantly checked and improved for effectiveness. Specifically, the Investments and Securities Act of 2025²¹ mandates the board of directors of a public company to report on the effectiveness of the company's internal control system in its annual report. This includes ensuring the integrity of the company's financial controls and reporting, which are crucial in cybersecurity.

The Exposure Draft of the Risk-Based Cyber-Security Framework and Guidelines for Other Financial Institutions, 2021, further outlines the board's role in cybersecurity governance particularly for other financial institutions.²² It emphasises that the board should ensure that cybersecurity is integrated with business functions and well managed across other financial institutions.²³ The

20 Why Untrained Employees Are Cybersecurity's Greatest Vulnerability. <https://www.e360.com/blog/why-untrained-employees-are-cybersecuritys-greatest-vulnerability>. The article is taken from Episode 26 of the State of Enterprise IT Security podcast.

21 Section 89 (2) of the Investment and Securities Act, 2007

22 Section 2.4 of the exposure draft

23 Section 2.4.3 of the Exposure Draft of the Risk-Based Cyber-Security Framework and Guidelines for Other Financial Institutions, 2021



board is also responsible for promoting a cybersecurity-conscious culture²⁴ and ensuring cybersecurity governance aligns with corporate and Information Technology governance.²⁵

Board responsibilities to ensure that adequate cybersecurity include the approval of cybersecurity budgets to ensure adequate investment in security infrastructure, monitoring compliance with global cybersecurity standards and frameworks, ensuring incident response plans are in place to mitigate the impact of potential breaches, overseeing third-party risk management, given that many breaches occur through vulnerabilities in vendor systems.

4. Adopting a Proactive Cyber Governance Approach

In order to be able to combat challenges associated with today's digital age in an optimal way, proactive cybersecurity governance by boards is imperative. The proactive approach will include shifting from being reactive in handling crises to being proactive in planning for risks.

This will entail carrying out periodical checks of the organisation's digital infrastructure to identify vulnerabilities and prioritise strategies to mitigation these risks. Emphasis which was once placed on the financial literacy of directions should gradually shift to cyber literacy as we are becoming more reliant on technology. Boards should be strategic about appointing directors who are tech savvy with cybersecurity expertise or setting up special committees to provide specific oversight.

There is also the need for boards to consider intensive technology retreats to deep dive into technology issues of great concern for organisations and train board members on emerging cybersecurity threats, regulatory changes, and best practices in risk management cannot be overemphasised. This will also entail engaging with regulators, fellow industry players, and technology providers to understand the prevalent cybersecurity threats and available solutions or defences.

It may be ignorant to expect an organisation to be totally immune from cyberattacks. However, having a board that understands cyber risk, puts in place a risk management framework that incorporates cyber risk and promotes a culture of cyber awareness will help to ensure the organisation's cyber resilience.

24 Section 2.4.2 of the Exposure Draft of the Risk-Based Cyber-Security Framework and Guidelines for Other Financial Institutions, 2021

25 Section 2.4.4 of the Exposure Draft of the Risk-Based Cyber-Security Framework and Guidelines for Other Financial Institutions, 2021



The board should ensure management integrates cybersecurity risks into their strategy and takes appropriate measures to manage this risk while promoting business agility and the ability to recover quickly from a cyber-attack. It is also the board's responsibility to ensure the safe and ethical use of this technology.

For example, the United States Securities and Exchange Commission (SEC) adopted new rules that require more cybersecurity disclosures from US-listed public companies in December 2023. By the rules, the US-listed public companies are required to disclose within four business days that they have sustained a material incident. Additionally, they are required to disclose risk management and governance information as related to cybersecurity in annual disclosures.

In Nigeria, by virtue of Section 21 (1) of the Cybercrimes Act, any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team ("CERT") Coordination Centre through their respective sectoral CERTs or sectoral Security Operations Centres ("SOC") of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues. In such cases, and in order to protect computer systems and networks, the National CERT Coordination Centre may propose the isolation of affected computer systems or network pending the resolution of the issues.

Similarly, section 40 (2) of the Nigeria Data Protection Act, 2023 ("NDPA") requires data controllers or processors, to notify the Nigeria Data Protection Commission ("NDPC") within 72 hours of becoming aware of a data breach incident. Unlike the US SEC rules that makes it mandatory for US listed public companies to not just disclose the incidence but risk management and governance information as related to cybersecurity, it is recommended that regulators also make it a requirement for companies, especially, to disclose their risk management mechanisms.

There is no doubt that it will be financially demanding to ensure an organisation has adequate cybersecurity mechanisms, but boards must, however, be determined to treat cybersecurity issues as a strategic investment and not as an operational expense. A proactive cybersecurity governance framework will ensure an organisation's resilience in the face of threats, safeguarding its assets and reputation while maintaining stakeholder trust.



5. Conclusion

Digital Transformations are significantly changing corporate governance processes. In the wake of technological disruptions, boards must establish frameworks prioritising strong cybersecurity and ethical technology adoption to navigate attendant issues. Corporate boards may handle new issues and provide doors for innovation and expansion by cultivating a culture of technological proficiency and aggressive involvement.

Similarly, the regulators also have a role in ensuring that there is a robust legal framework guiding the integration and use of technology in business operations. In this age of digital revolution, corporate governance must serve as a stabilising force, preserving resilience, accountability, and trust in a world growing more interconnected by the day.

AUTHOR



Abasiemediong Etuk, MCArb
*Corporate Governance and
Regulatory Compliance Unit*



Contact

LAGOS

Kenna Place
8, Ogunyemi Road, Palace Way, Oniru
PO Box 73002, Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285, Abuja

ENUGU

3 Emmanuel Ngwu Street,
Thinkers' Corner,
Enugu, 400001

+234 811 395 1052, +234 811 395 1053
counsel@kennapartners.com

