BANK OF INDUSTRY
...transforming Nigeria's industrial sector

INSTITUTE OF CHARTERED SECRETARIES AND ADMINISTRATORS OF NIGERIA

KEYNOTE ADDRESS
AT THE
INSTITUTE OF CHARTERED SECRETARIES & ADMINISTRATORS OF NIGERIA (ICSAN)
CORPORATE SECRETARIES AND REGISTRARS FORUM
2024

Topic: The Implications of Cybersecurity and Artificial Intelligence on Capital Market Operators

Date: March 2024

Distinguished Ladies and Gentlemen

It is my distinct honour and pleasure to be here to present a keynote address at the 2024 ICSAN Corporate Secretaries and Registrars Forum. The theme of this year **"The Implications of Cybersecurity and Artificial Intelligence on Capital Market Operators**" is indeed significant especially in today's interconnected world due to the increasing reliance of businesses and organisations on digital transformation. I am confident that the combined experience and leadership of the professionals here today can continue to propagate excellence toward the sustainable growth of the institute.

The advent of Artificial Intelligence (AI) has brought about substantial changes in both personal lives and various industries globally. Its transformative impact is evident in revolutionizing processes and boosting efficiency. The financial sector is no stranger to this evolution, as AI has reshaped the delivery of financial services, paving the way for innovative products and solutions.

The advancements in AI technology have permeated every facet of the capital market industry. From front-office tasks such as liquidity searches to back-office functions like error reduction and automation, AI has become deeply integrated. Promising remarkable enhancements in efficiency, accuracy, and decision-making processes, AI stands poised to redefine the landscape of financial services.

As you may rightly know, the capital markets around the globe are the most data-sensitive segment of the financial industry and AI is reshaping how traders, investors, and financial institutions perceive, analyse, and interact with the markets. Based on the report by Deloitte, AI has the potential to democratise access to capital across the global economy thus increasing its efficiency, safety, and performance.

AI undoubtedly offers significant benefits, particularly its role in positively transforming the capital markets, however, individuals and organizations are continually dealing with the associated risks. According to the latest National Cyber Threat Forecast report there is an upsurge in insider threats through impersonation scams with an increase in the use of Artificial Intelligence (AI) for malicious purposes.

In recent years, the capital markets have witnessed a surge in diverse investment opportunities, with massive support from private sector institutions in collaboration

with the Federal Government. The integration of new and innovative technologies has resulted in increased economic activities, while also making the markets susceptible to cyberattacks.

Currently, Nigeria's capital market is expected to reposition the economy along a path of sustained growth by broadening asset classes, improving liquidity, and deepening transactions. The more investments that come into the market, the better the economic growth and development outlook. Accordingly, proactive measures must be put in place to safeguard the volume of transactions in the markets.

For the Nigerian capital market to harness the advantages of AI, individuals must cultivate a culture of cybersecurity literacy; align specific metrics for cyber risk management, and increase the pace and substance of ongoing strategic risk management. Corporate governance presents an opportunity for board members and top management to continually refine their communication skills, bringing cyber-literacy to the boardroom, and enhancing their organization's cyber resilience.

Some of the impacts of AI and cybersecurity practices in capital markets include:

AI in Capital Markets:

- **Algorithmic Trading:** AI algorithms are used to analyze vast datasets and execute trades at high speeds based on pre-defined parameters.
- **Fraud Detection:** AI can analyze transaction patterns to identify suspicious activity and prevent fraudulent transactions.
- **Risk Management and Compliance Automation:** AI can assess complex financial instruments and market conditions to help capital market operators make informed risk management decisions. AI can facilitate automation risk management processes, such as counterparty credit checks and cybersecurity measures.
- **Portfolio Management:** AI can create and manage investment portfolios based on individual client goals and risk tolerance.
- **Straight-Through Processing:** AI-driven automation enables straight-through processing to ensure seamless and efficient trade execution, minimizing errors and delays.

- **Cost Reduction and Operational Efficiency:** One of the key advantages of embracing AI in capital markets is the potential for cost reduction and operational efficiency.
- **Advanced Analytics and Decision-Making:** AI equips firms in the capital market with sophisticated analytical tools, sharpening their ability to base decisions on data with improved precision and accuracy.

Cybersecurity in Capital Markets:

Distinguished participants, it is important to note that Cybersecurity is the practice of protecting internet-connected systems against cyber threats. The threats imposed on firms operating within the capital market are huge, given the continued improvement in information technology and other digital as well as mobile internet channels, which make the market susceptible to cyber risk.

Our market is exposed to two major cyber risks:

- The first is the ***direct operational and financial loss impact*** of successful cyber-attacks.
- The second is the indirect effect of such exposure to the market ***reputational and financial penalties*** resulting from the market regulators.

However, either of the two effects will result in the following for organisations:

- ✓ Eroding financial performance
- ✓ Identity theft
- ✓ Reputational damage
- ✓ Legal repercussions for the market
- ✓ Loss of trust from investors
- ✓ Loss of intellectual property, among others

Colleagues, all hope is not lost, as there are preventive strategies for individuals, firms and the general society as a whole - to prevent and mitigate the impact of cybercrime. I will separate these as follows under three main sub-headings:

Individual preventive measures

- ✓ Create strong passwords and use two-factor authentication

- ✓ Keeping software and operating systems up-to-date with the latest security patches.
- ✓ Avoid using public Wi-Fi networks and a Virtual Private Network (VPN)
- ✓ Be cautious of suspicious emails and messages.
- ✓ Backing up important data regularly
- ✓ Get updated about cybersecurity threats and best practices often.
- ✓ Quick and timely incident reporting of any attempt of cyber-attacks.

Business Organisation prevention and Mitigation measures

- ✓ Conducting regular security risk assessments
- ✓ Implementing access controls and monitoring for suspicious activity
- ✓ Providing cybersecurity training for employees
- ✓ Implementing strong passwords, two-factor authentication, and encryption for sensitive data
- ✓ Incident Response Planning**.** This involves having a clear plan for identifying, containing, and recovering from cyberattacks is crucial.
- ✓ Cybersecurity Awareness Training: This practice educates employees about cybersecurity best practices to minimize the risk of human error.
- ✓ Implementing a robust backup and disaster recovery plan
- ✓ Zero Trust Architecture**:** This approach assumes no user or device is inherently trustworthy and verifies access continuously.
- ✓ Regularly updating software and hardware systems.
- ✓ Constant Implementation of the Regulatory Compliance framework.

Economy-wide Measures

- ✓ Establishing cybersecurity standards and regulations for businesses and organizations.
- ✓ Providing resources and training for individuals and businesses on cybersecurity best practices
- ✓ Investing in research and development of new cybersecurity technologies and tools

- ✓ Enforcing penalties for cybercrime and holding perpetrators accountable
- ✓ Sharing threat intelligence and collaborating with international partners to combat cybercrime globally.

Distinguished colleagues, as we look forward to a cyber-secure future, driven by technology and innovation, there will be opportunities as well as challenges in our day-to-day operations. However, we are presented regularly with more tools to combat the threats as they arise. Leveraging advanced technologies, fostering global collaboration, and prioritizing cybersecurity education and awareness can mitigate risks and ensure a secure digital future. What is very clear is that it is increasingly important to stay ahead in the ever-evolving world of AI and cybersecurity.

Before I conclude my presentation, I will briefly talk about the role of the Bank of Industry in supporting enterprises in the country. BOI's mandate is to provide financial assistance for the establishment of large, medium, and small projects; as well as the expansion, diversification, and modernisation of existing enterprises; and rehabilitation of moribund ones. In line with this mandate, we play a significant role in supporting Nigerian businesses by providing innovative financial support (mostly through single-digit interest rates, long tenor, and a reasonable moratorium period). Between 2015 and December 2023, the bank provided financing of over ₦1.95 trillion to enterprises across different sectors of the economy.

Other BOI interventions beyond finance:

The bank collaborates with Business Development Service Providers (BDSP) to provide business advisory services (e.g. capacity building, mentoring, business model design, business plan creation, entrepreneurial training services, etc.) to MSMEs. Since 2014, the bank has partnered with over 300 BDSPs to support MSMEs across the country.

The bank regularly sponsors local and international industry trade fairs that target the promotion of locally manufactured goods and services such as the Lagos Leather Fair, Fashion Souk, etc. BOI is also a member and on the Steering Committee of the National Action Committee on Africa Continental Free Trade Agreement (AfCFTA) in Nigeria, and has offered a lot of input into shaping Nigeria's response to AfCFTA from a policy perspective as well as offering practical support

to our customers. We have also collaborated with AfDB, Afreximbank, and other stakeholders on the establishment of Special Agro-Processing Zones (SAPZs) and Special Economic Zones (SEZs).

Funding – The bank provides funding for the digital economy through financing broadband telecoms infrastructure, database and storage centres, etc.

Fintech for micro loan disbursement – BOI under the Microenterprise Directorate supports organisations with financial technology platform to disburse loans to micro businesses.

Investment in Digital and Creative Enterprises (I-DICE) Fund – The Bank is the implementation agency for the AfDB US$617.7 Million Investment in Digital and Creative Enterprises (I-DICE). The objective of the program is to promote entrepreneurship and innovation in digital technology and creative industries to support the government's job creation efforts, especially for young people.

Cyber Security Desk – The Bank ensures that staff awareness is carried out periodically on cyber security threats in the digital space and also implements measures to ensure that the Bank's digital assets are protected.

In closing, I urge us all to continue to espouse the ideals of this great institution and be worthy ambassadors. In today's world, corporate governance is key to ensuring that organizations are managed on a sustainable basis. I am confident that if we all play our part, we will be able to build a Nigeria that will provide decent opportunities and improve the quality of living for its citizens.

Thank you for your attention.