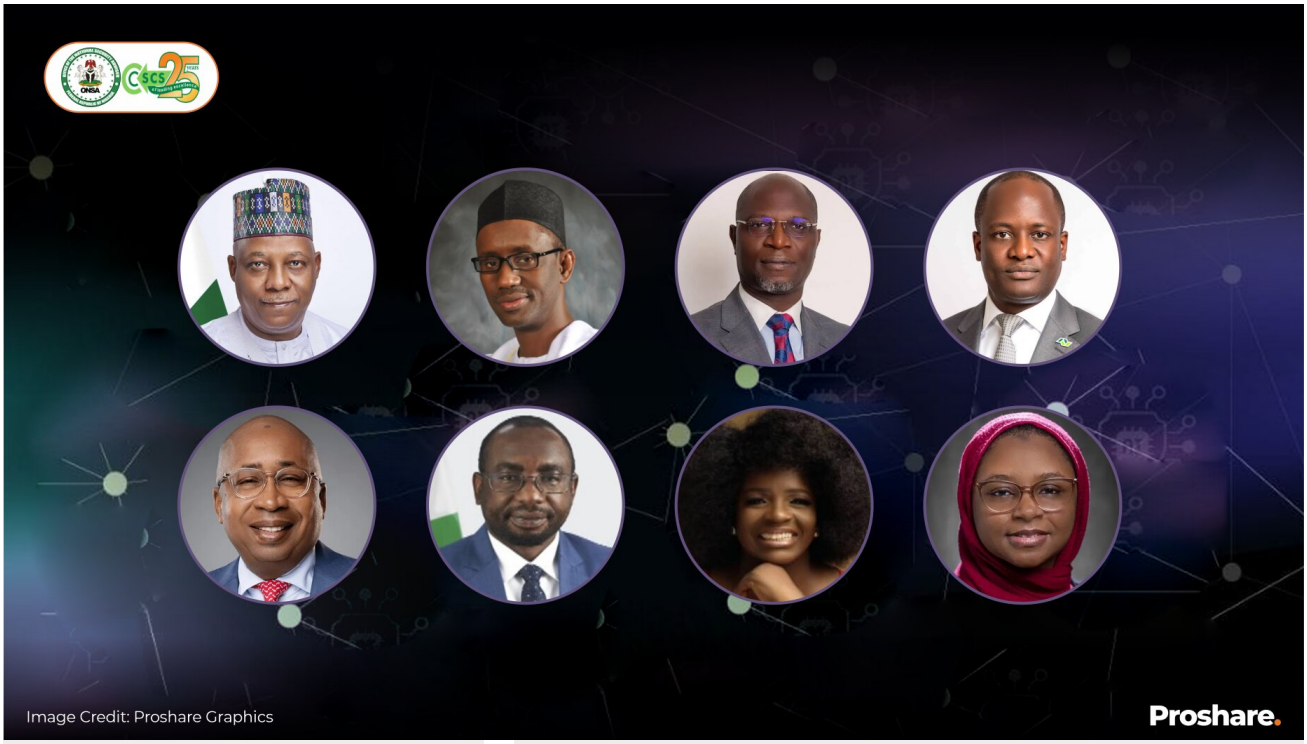
The Analyst™ Note.

The Rapporteurs Report on The Cybersecurity Conference 2024: Cybersecurity Synergizing AI and Infrastructure.



Issue Date:
Wednesday, December 4, 2024

A Market Intelligence and Strategic Advisory Group Report

Production:
Proshare Graphics.

Being the rapporteur's report on The Central Securities Clearing Systems Plc (CSCS) Cybersecurity Conference 2024 held in collaboration with the Office of the National Security Adviser Themed Cybersecurity: Synergizing AI and Infrastructure held at Transcorp Hilton Hotel, Abuja, on October 17, 2024.

1. Executive **Summary.**

The 2024 Central Securities and Clearing Systems Plc (CSCS) Cybersecurity Conference considered the theme ***Cybersecurity: Synergizing AI and Infrastructure***. The conference brought together key stakeholders from the public and private sectors and security agencies. Following a fireside chat, the conference featured four panel sessions and eight presentations. Participants collectively acknowledged that although technological innovations and advancements in artificial intelligence offer significant opportunities, there is a considerable shortfall in essential digital infrastructure, regulatory frameworks, and the requisite skills to harness these advancements and proactively address potential misuse effectively. As a result, cyber threats continue to pose a persistent challenge. Ik Osakioduwa was the event compere.

This report is presented under the following headings:

- Address by Key Stakeholders
- Key Insights from the Fireside Chat
- Presentations and Key Views Across Plenary Sessions
- Simulation Attack Presentation
- Raffle Draw and Outcome

- Closing REMARKS
- Conclusion
- Key Takeaways
- Appendix

2. Address by Key **Stakeholders.**

Welcome Address by Mr Temi POPOOLA, Chairman, Board of Directors CSCS Plc

The conference commenced with a welcome address by Mr Temi Popoola, Chairman of the Board of Directors, CSCS Plc. The speaker welcomed all attendees to the fifth CSCS conference, organised in partnership with the Office of the National Security Adviser (ONSA) as Co-host. The Chairman noted the timeliness and critical nature of the 2024 Cybersecurity conference theme, noting the increasing capacity of a single cyber-attack or cybercrime to disrupt nations and the projected annual cost of approximately $10.5trn.

Ai's predictive capabilities and lightning-fast response present an opportunity. However, Mr Temi noted AI's ability to introduce unprecedented risks. The sobering statistics and costs that could result from AI's duality of opportunity and threat amidst cybercrime concerns emphasize the increasing need for collective engagement and contributions by all stakeholders in a bid to harness AI's power to build secure digital ecosystems, balance innovation and security, and shape the future.

Goodwill Message by Dr Emomotimi AGAMA, DG, Securities and Exchange Commission (SEC)

"*Cybersecurity is not merely a technological issue; it is a strategic imperative.*"- Emomotimi AGAMA.

The SEC DG described the Cybersecurity Conference as **timely** and even more **critical** today than previously envisaged in driving awareness/education and bringing to light the most pressing issues within the space. The speaker noted that cybersecurity is no longer an isolated concern but has become rooted in the socio-economic systems across global economies and markets. Technological disruptions such as AI have resulted in **efficiencies;** however, they have also brought cyber risks that must be recognised and guarded against to preserve and maintain the trust and integrity of the capital and financial markets. Real estate market trends.

Precedents such as the COVID pandemic accelerated reliance on technology, remote work, and digital platforms emergence increased the need for measures/infrastructures to enhance cybersecurity measures and protect individuals, organisations, and sectors from threats in cyberspace. Robust cyber risk strategies and infrastructures are thus desired as a critical component in sustaining financial stability and national security. The SEC head noted the importance of greater collaborations and partnerships, such as those witnessed between CSCS and ONSA. Additionally, the speaker noted the place of emerging Intelligence, such as AI, playing a key role in the fight against cyber threats while offering the capability to monitor vast data, speedy analytics and accuracy, and reduced time of monitoring fraud incidence/ threats and response.

The speaker notes the SEC's commitment in ensuring that the capital market is protected by robust cybersecurity frameworks that balance innovation with accountability. Additionally, AI holds great promise. However, it must be complemented by the proper infrastructure. According to the SEC DG, "Where infrastructure is still developing, security must be integrated at every layer from communication networks to data centres." The SEC DG described the CSCS as the Nigerian capital market's world bank. Its protection requires the collaboration of all stakeholders to secure a resilient digital environment capable of withstanding emergent threats.

Conference Opening Address by Ahmed SAAD ABUBAKAR, National Cybersecurity Coordinator, ONSA

Mr Ahmed Saad emphasised that maintaining critical infrastructure was the role of every stakeholder and that the best approach is a whole-of-government and whole-of-society approach. According to the speaker, two transformative forces can be observed in current trends in Nigeria: the rapid emergence of AI and the growing need to secure national assets as reliance on digital infrastructure has increased vulnerability to cyber-attacks. AI emergence presents both challenges and opportunities. The challenge is that technology users will never know when they will be hit; however, they could also serve to protect and coordinate the fight against cyber threats and cybercrime activities.

Mr Ahmed highlighted the efficiency that could be derived from proactive measures to curb cyber

risks. The speaker recalled the positive outcomes derived through the EFCC's fraud forums prior to the emergence of the Cybercrime Act. The speaker noted that during this period, banks were not mandated to report incidence of cyber attacks. Still, the evolving cyber regulatory provisions and the emergence of the Cybercrime Act mandated that all critical information infrastructures disclose all cybercrime incidents to the Nigeria Computer Emergency Response Team (NCERT) or face sanctions.

In 2024, upon the ONSA's recommendation to the President, key infrastructures have been designated and gazetted as critical national information infrastructure (CNII) within the ambit of the Cybercrime Act 2015. Due to the need for a protection plan for these CNII's, collaborative efforts between public and private agencies must be geared toward developing a national protection plan for these assets.

Going forward, the ONSA will host a workshop on CNII's on October 28-29, 2024, to discuss/examine the gazette and develop a clear mandate on processes and procedures to protect Nigeria's Critical National Information Infrastructures. Finally, the speaker commended the collaboration between CSCS and ONSA, noting the need for greater cooperation by all stakeholders to protect critical infrastructures to curb cybercrime.

Keynote Address by Haruna Jalo-Waziri, Managing Director/CEO, CSCS Plc

"*Our collective knowledge is our greatest asset*" - **Haruna JALO-WAZIRI**

Following Thomas Murray's cybersecurity ratings, CSCS moved to lead the way towards digital infrastructure protection by extension, scaling up and automating cybersecurity processes, which it has commenced by virtue of its Cybersecurity Week and Cybersecurity Conference 2024. The CSCS MD expressed special appreciation to all partners, attendees, and the CSCS team. The CSCS MD also appreciated the partnership and collaboration between CSCS and ONSA, the conference's co-host.

Navigating deeper into the 21st century, new vulnerabilities have emerged in technological advancements presented by the information age. Mr Jalo-Waziri notes that technological advancements can be powerful allies or dangerous adversaries. The potential of technologies such as AI must thus be harnessed; however, threats must also be considered. Citing the 2024 Cybersecurity Ventures report, the speaker noted that global cybercrime damage costs are projected to reach $10.5trn by 2025, up from $3trn in 2015, underscoring the need for robust cybersecurity measures. A report by Checkpoint Research reveals that ransomware attacks have risen by 45% in 2024. The Nigerian cyberspace landscape has remained challenged, with businesses facing an average of 2650 cyber attacks weekly.

Protecting digital infrastructure has become paramount with the increased reliance on digital systems. The cybersecurity infrastructure agency notes that practical implementation can predict and prevent cyber attacks. The speaker notes that the intrusive impact of social media, capable of amplifying cyber threats, must be considered in decision-making. Trusted networks with diverse expertise and air gaps must be created to foster a more resilient cybersecurity network. According to the CSCS MD, the intrinsic value of human intelligence should not be forgotten. More efforts should be geared toward understanding cyber risks and taking proactive measures to curb these risks.

H.E. Kashim SHETTIMA GCON, Vice President of Nigeria

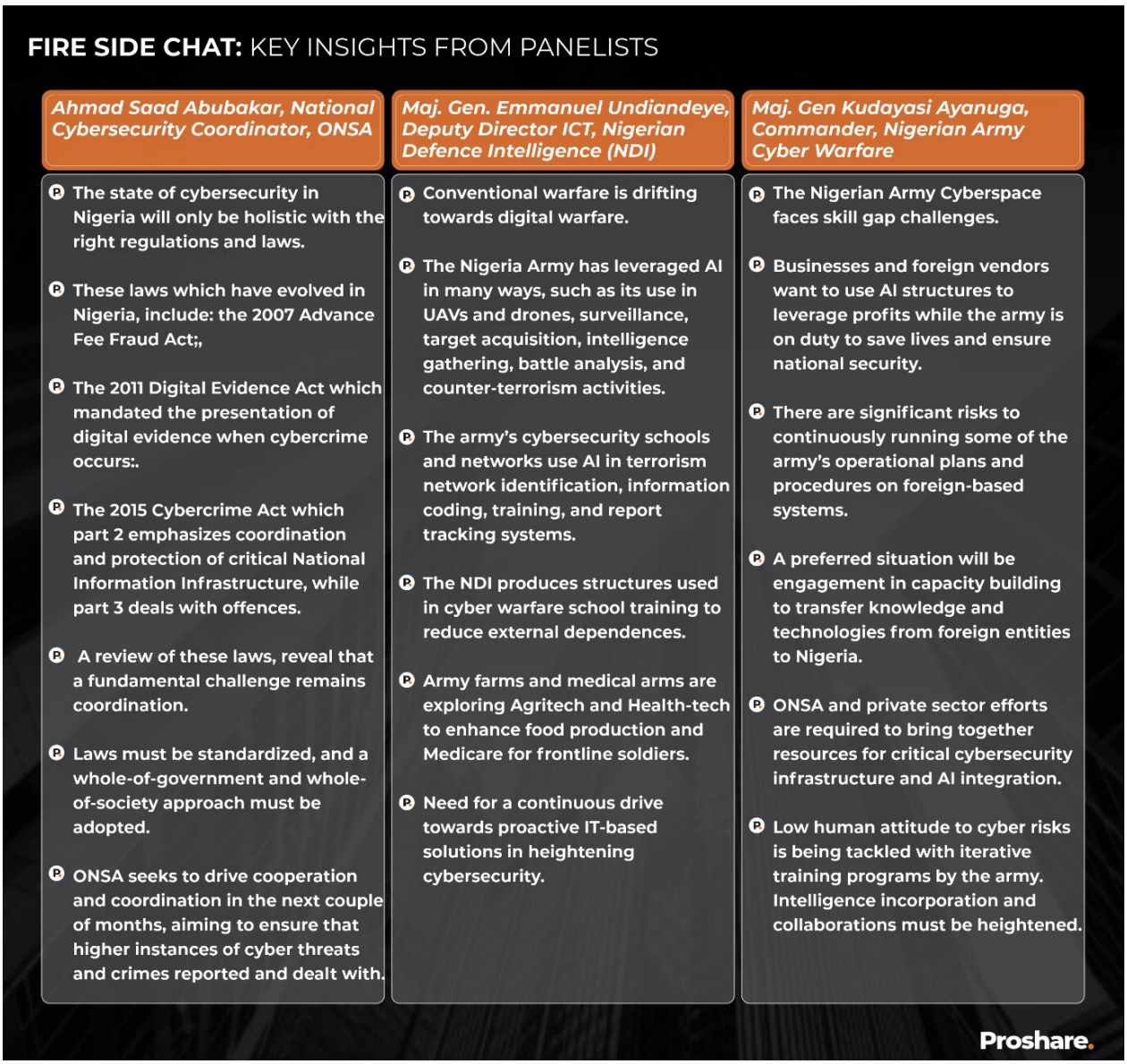
"*The task ahead is clear: to guide the expansion and utilisation of AI within a resilient, secure future.*"- **Kashim SHETTIMA**

The Vice President delivered a welcome address via pre-recorded video message. Mr Bashir Mohammed Shuaibu, the special assistant to the President on ICT Systems and Digital Skills, who represented the vice president and delivered the speech, noted that AI speaks to the heart of the industrial revolution, and its potential can only be harnessed if infrastructures are optimised.

The convergence of AI and critical infrastructures presents enormous opportunities and poses unprecedented security risks. The risks could be associated with bad actors that leverage AI to launch sophisticated cyber attacks. The vice president asserts that the solution lies in building a robust, secure foundation for AI. As AI becomes the backbone of modern infrastructure, its security must be paramount. To mitigate cyber threats, cybersecurity must be embedded in every level of AI-driven security systems. The vice president adds that ethics and trust must be at the forefront of every AI security system with the proper governance framework.

3. Address by Key **Stakeholders.**

Technology has become rooted in the functioning of all critical infrastructures, and recent years have seen military and defence structures face an evolving cyber risk demanding a stronger and coordinated response. The panel session, moderated by **Ibukun ADEBAYO, Co-Founder and Director of Restitution Capital**, broadly considered "***the state of cybersecurity in Nigeria*** and key challenges in Nigeria's cyber landscape.



4. Presentations and Key Views from the **Plenary Sessions** (Breakout Rooms).

The conference featured eight presentations and four plenary sessions

Presentation 1: ***Harnessing the Power of Artificial Intelligence in Your Cyber Security by Yemi KERI, CEO Hackerbella Limited***

The presenter highlighted the increased adoption of technology and devices in Nigeria, which has seen organisations' increased reliance on data. Data must be protected, and in Nigeria, a lot remains to be done around data protection. Third-party integration of systems by organisations must be done, noting the level of security structures/systems of such APIs used in integrations, and data encryption must be ensured.

On strategies for enhancing cyber security, the Hackerbella CEO emphasised the role of management and the board in putting in place matrices that ensure proactive structures are in place while leveraging AI. In leveraging AI strategy

for cybersecurity, the CEO notes that AIs have been trained and are capable of revealing patterns that guide informed decisions. The power of AI must thus be leveraged to enhance cybersecurity in organisations.

Harnessing the power of AI ensures early threat detection through AI isms, predictive analysis, AI-based phishing, and cloud security, among other things. Board and management must ensure strategies that embed AI into organisations' cyber security strategies.

***Presentation 2:** Cybersecurity and AI: Enabling Security While Managing Risk by Adedoyin ODUNFA, CEO Digital Jewels*

The presenter, describing AI as a double-edged sword on steroids, explained that AI's dual potential could transform the business and the wealth of nations; however, it also presents increased risk, cost, and competition disadvantage. The impact of IT is evident in the top ten most valuable brands globally, which are all IT-enabled. Digital leaders are, therefore, found to perform better than digital laggards as IT was seen to improve performance across organisations.

The presenter describes IT as the game changer but AI as the game changer on steroids. Stressing AI's benefits, the presenter stated that AI helps to improve efficiency, aids medical advances, promotes creativity, aids better decision-making, creates business opportunities, promotes device personalisation, and impacts the environment. AI applications in cyber security extend to identifying and predicting possible breaches, faster incident response, managing vulnerability, quick analysis, fraud detection, and cloud security.

Relative to AI's possible risks and challenges in cybersecurity, the CEO identified bias and ethical concerns, large data requirements, skills gaps, and regulatory considerations. On the dangers in the AI pipeline, the CEO identified data collection and handline, model training, systems architecture, and model inference.

According to the presenter, the challenges between the promise and AI mean there will be more phishing campaigns; however, AI can also boost cyber security and give precise predictions.

***Presentation3:** State of Exploitation across the Internet by Dr. Obadare Peter ADEWALE, Founder & CEO, Digital Encode*

AI is revolutionising systems and operational modes, presenting both opportunities and risks. Due to AI's dual possibilities, Dr Obadare describes "the state of the internet today as one of the good, the bad, and the ugly." The Dr notes that cyber threats and electronic fraud are two monsters fighting cybersecurity and destroying the internet experience of users and organisations.

Systems are increasingly being digitally invaded, and the cybercrime economy has become the third-largest economy today. Analysts project that the next global crisis will be a cyber pandemic. The presenter showed that any system can be digitally invaded, implying that the architecture, design, implementation, and operation of an innovation may falter due to vulnerabilities. Organizations should consider risks internally and externally. The CEO states that no matter how novel a technology is, there will be a digital invasion if security is not built into it.

The Digital Encode CEO gave examples of OpenAI, which was digitally invaded; Maersk, which suffered a ransomware attack that cost it over $300m; and an unnamed Hong Kong firm, which suffered a $25.5m loss due to a deepfake attack. These vulnerabilities come in different forms. One method to monitor for breaches is using the website haveibeenpawned.com, where the presenter encouraged users to enter their emails to check for incidents, noting that a red indicator would signify a breach.

The presenter advocated for fostering digital trust in the cyber intelligence quotient and having the right skills and technologies, noting that protection is about people, processes, and technologies. The CEO concluded that there is a need to build digital trust IQ to ensure zero or minimal cyber-attack vulnerabilities.

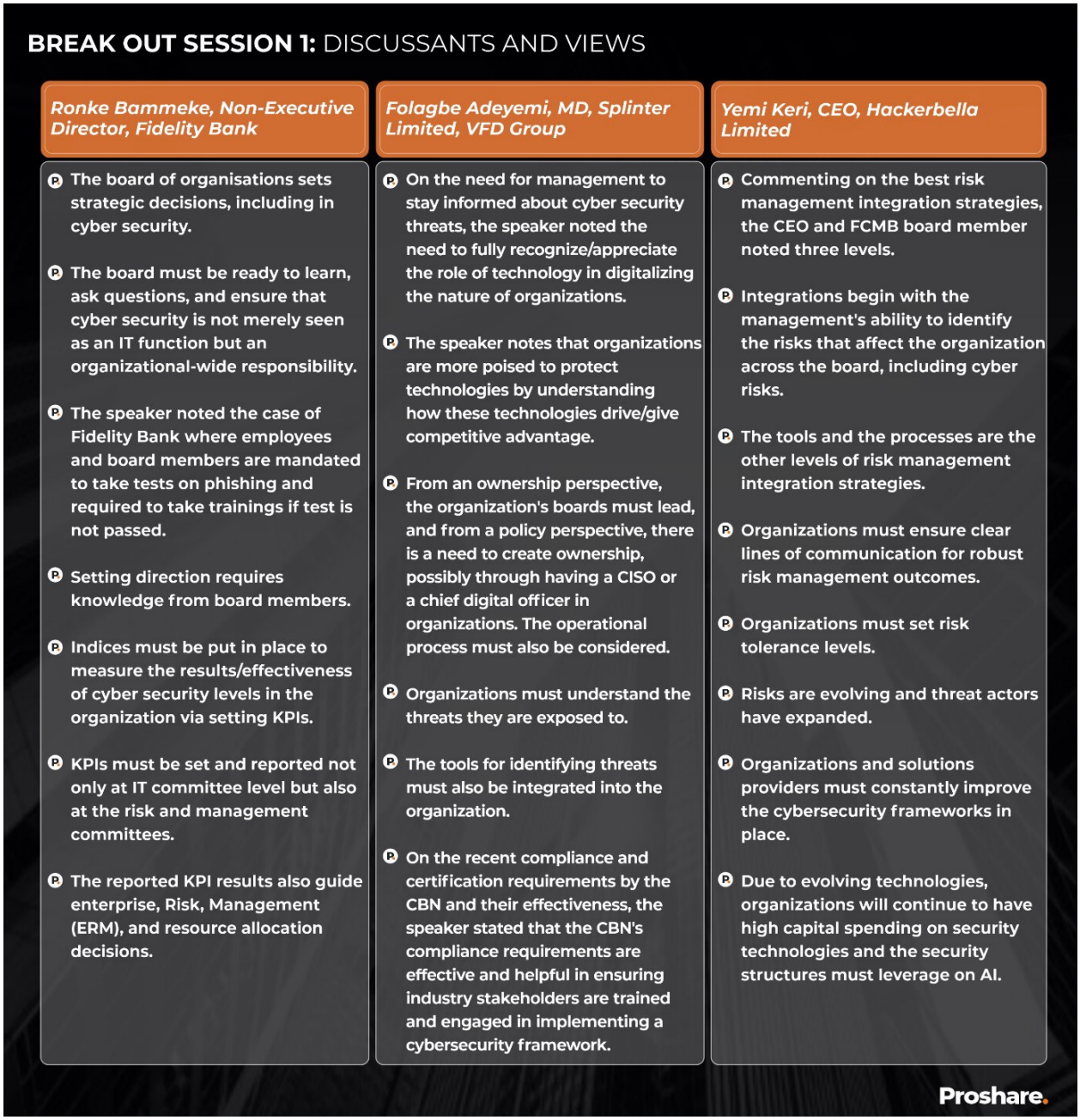
***Presentation 4:** Talent In the Age of Cyber Security and AI by Iyinoluwa BOYEJI, Co-Founder, Future Africa*

Following personal experiences with cyber attacks and actions taken to curtail such threats, the presenter discussed how the Hustle Kingdom has consistently contributed to increasing cyber-attacks.

The presenter states that Cybercrime in Nigeria has moved from a crime to a culture. The presenter advocates for creating measures/means of turning these talents into an opportunity and converting them to cyber analysts/cyber warriors, which will promote breakthroughs in several investigations and give them a better life after a life of crime.

Plenary Session

The first break-out panel session, moderated by ***Dr. Obadare P. ADEWALE***, Founder and CEO of Digital Encode, broadly considered "*The State of Exploitation Across the Internet.*"



The second break-out panel session, moderated by **Tobe NNADOZIE**, Divisional Head of Business Technology and Digital Innovation at CSCS Plc, focused on "***Expanding Attacks Surface: How AI has Impacted this.***"

Presentation 5: ***Building Resilient Financial Systems: AI's Role in Cyber Defence and Incident Response by Aisha ALI-GOMBE, Director, Cybersecurity Clinic, NSA, United States.***

Increasing adoption of technologies requires the integration of cyber resilience frameworks. The presenter describes cyber resilience as the ability of institutions and infrastructures to adequately put in defence

mechanisms to protect themselves against threats, rapidly respond to threats and recover rapidly using advanced technologies. To be cyber resilient, organisations must adopt best practices and compliance and ensure a culture of collaboration, information sharing and education of the workforce. The presenter showed that intrusion is at the top of threat incidents in the global cyberspace system, while in Nigeria, social engineering emerged as the biggest threat.

The presenter noted that achieving absolute cyber resilience may be difficult; however, the goal of risk and disruption minimisation must be a priority. Highlighting findings from a 2024 IBM report revealed that about 3000 cyber incidents were recorded in 2023, up from 1800 in 2022. Over 1000 data disclosure cyber incidents impacting about 1000 institutions and 16mn users were recorded. The IBM data also revealed that the health and finance sectors were among the top 5 most vulnerable. Further data revealed that about 1.3mn phishing attempts were recorded in the banking sector in Nigeria in 2023.

On leveraging AI to optimise processes and enhance security, the presenter notes that the AI landscape contains algorithms specific to cyber security, such as anomaly detection, adaptive models, predictive models, clustering, and classification systems. These models/algorithms can be applied to enhanced cyber security through insider threat detection, anomaly detection plus clustering to find malicious activities, phishing detection, EDR and NDRs.

The presenter notes that cybersecurity is a collective issue and must not be dealt with in isolation. Organisations must engage in collaborations and intelligence/information sharing. On the challenges AI poses despite its applicability to cyber security, the presenter outlines scrutiny of the actual AI system, which can be vulnerable, AI's ability to make wrong decisions, skill gap/knowledge, ethics, data privacy concerns, and regulatory challenges.

***Presentation 6:** Leveraging AI in the Advancement of Cyber security – by Bello HAYATUDEEN, Director, Crisis Sector, ngCERT.*

The ngCERT director introduced ngCERT and its mandates, such as developing and implementing policies that leverage opportunities from technologies such as AI. The ngCERT proactively seeks to use AI to detect and examine attack patterns and provide significant and proactive responses to threats across diverse sectors, such as defence and finance.

The speaker affirms that AI's advantages include, but are not limited to, threat detection, automated responses to threats, predictive analysis, resource optimisation, enhancing human skills, development of network security potential, identity management, phishing detection, user behaviour analytics, and threat intelligence.

The speaker adds that the president's critical infrastructure protection executive order is in force. The speaker notes that the president's executive order on designating identified infrastructures across 13 sectors with national status requires a protection plan, and ngCERT was among the key developers of such a plan.

According to the speaker, Nigerian cyberspace still faces challenges in leveraging AI, notably in issues related to data privacy, and skills gaps persist. In conclusion, the speaker notes that AI is an enabler, not a threat, emphasising the role of R&D in promoting security.

Question from an attendee/cyber security enthusiast (Elizabeth AKUSA): Given recent bank network service failures, are there ways to mitigate the risk of cyber glitches?

Answer: No report of infrastructure hack has been received by any banks. ngCERT, however, does not fail to act on all reported incidents.

***Presentation 7:** Proactive defence through rigorous crisis management by Collins ONUEGBU, Chairman, Signal Alliance Technology Holding and Bamidele OGUNMAKIN, Cybersecurity Architect – Microsoft Security Enterprise Services.*

The presentation focused on national infrastructure security. The presenters showed that cyber attacks on public infrastructures have doubled in the last two years. Attackers are increasingly using AI to attack. The presenter revealed that in 2024, about 65trn signals were detected and analysed by Microsoft. Microsoft is noted to have increased its investment in security experts training in 2024 and tracked 1,500 threat actors in 2024 relative to 300 in 2023.

However, organisations have expressed challenges in responding to attacks, including a lack of clear guidance on how to respond, a limitation in the number of devices protected, a large volume of attacks undermining proactive measures in place, and creating synergy in orchestrating a response with other organisations.

With respect to what can be done to prevent attacks, the presenters advocated for preparation through proactive measures, communication and awareness, execution, and a playbook on how to respond should be in place. From a cyber security point of view, the most important of these actions are to protect identities, protect device identities, protect data, and automate response strategies. In conclusion, the presenters noted the possibility of the strategy to work with a modern security operation centre at the top.

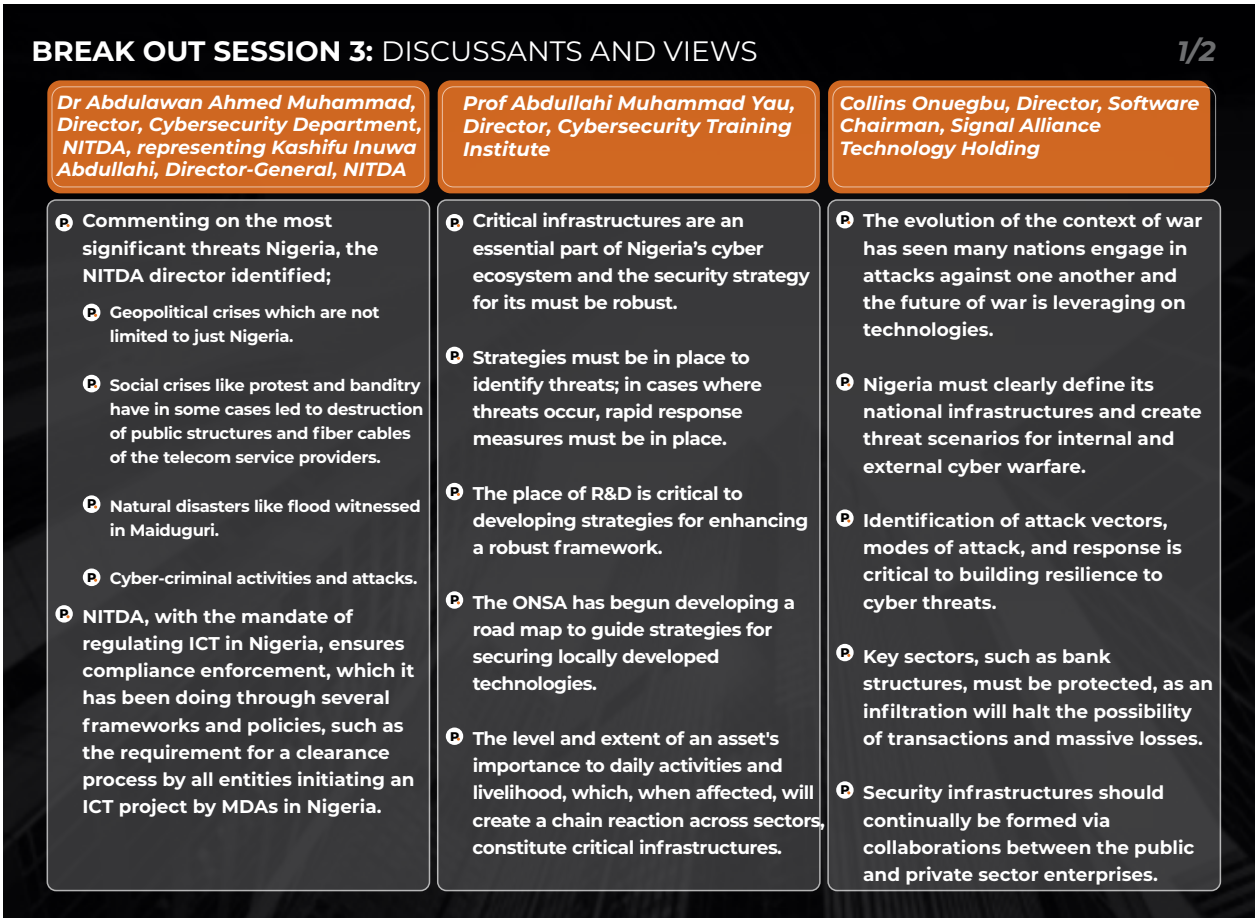
***Presentation 8:** Mitigating AI parallel attacks on critical infrastructure strategy for security- By Jimi FALAIYE*

Mr Jim Falaiye focused on protecting assets/devices and infrastructures that have become integral to firms' operations. Certain AI that power malware can adapt to real-time scenarios, prompting attacks on organisations. The scale of AI-powered attacks raises concern, as recent events have seen a single-source attack affect global operations.
The speaker noted AI's ability to analyse large amounts of data. If weak spots are not identified, threat actors can identify and exploit possible vulnerabilities. Data manipulation and tampering using AI affect individuals' and organisations' decision-making.

In mitigating threats, Mr Jimi advocated for continuous assessment of cyber security levels, resilience, threat modelling, integration of several defence layers, segmentation to limit attack spread and contain breaches, industry collaboration, the need to adhere to standards, continuous monitoring, and proactive response systems.

The speaker concludes by noting that people are the weakest link to cyber security, thus the need for constant personnel training and awareness by organisations. Organisations must also have cybersecurity drills, such as phishing drills, as attack response measures.

The third break-out panel session, moderated by **Aisha ALI-GOMBE**, Director of Cybersecurity Clinic, NSA, US, focused on the topic "Critical Infrastructure Protection and International Coordination."



2/2

Dr Abdulawan Ahmed Muhammad, Director, Cybersecurity Department, NITDA, representing Kashifu Inuwa Abdullahi, Director-General, NITDA	*Prof Abdullahi Muhammad Yau, Director, Cybersecurity Training Institute*	*Collins Onuegbu, Director, Software Chairman, Signal Alliance Technology Holding*
The NITDA also has policies related to content development, cloud computing, and blockchain technology usage. The NITDA ensures that its policies meet global standards. On measures to fill the skill gap in Nigeria's cyber security landscape, the NITDA cyber security department organizes an annual cyber security challenge in a bid to identify talents. Nigeria also scaled third place in the recent ECOWAS cybersecurity hackathon.	The ONSA has different threat actors across different fields, which work to identify internal and external threats to critical infrastructures. The ONSA is designing a protection plan for several critical infrastructures in the economy, collaborating with other critical stakeholders. Protection plan development will be an activity of focus at an event by the ONSA in the week ahead. Commenting on international collaborations on digital information/ intelligence sharing, the ngCERT engages in collaborations and intelligence sharing with other nations on cyberspace activities.	Collaborations should begin right from where projects are conceptualized. The public sector must provide adequate regulatory guidelines to enable the private sector enterprise activities, promote industry growth and protect users of products and services. Nigeria needs to align its education system with its cyber skills needs, identify the number and type of experts required and measure to deploy training within a specified period.

Proshare.

The fourth break-out panel session, moderated by **Bello HAYATUDEEN,** Director, Crisis Sector, ngCERT Consulting Ltd, focused on "***Cyber Intelligence as a Defending Fortress.***" The session revealed that cyber security is the cornerstone of national security, enabling governments to identify and mitigate threats, protect critical infrastructure, and formulate strategies. While challenges remain in implementation, the mandate of sage guarding national interest cannot be overstated.

BREAK OUT SESSION 4: DISCUSSANTS AND VIEWS

1/2

Frederik Soendergaard-Jensen, COO, LIFU Technologies, South Africa	*Jimi Falaiye, Regional Manager, West Africa & Tanzania-SOPHOS*	*Ifeanyi Uche, Nigeria Police Force, National Cyber Crime Centre*
Being a Danish national, Mr Frederik noted the level of cyber threats Denmark receives from Russia due to its support to Ukraine. Through proactive cyber intelligence structures by the Danish cyber force and constant awareness activities to citizens, threats are contained Citing IBM cyber threat data, the speaker pointed at the growing number of threats and critical vulnerabilities and how the weaponization time of some critical vulnerabilities is now limited to just 8 days.	The SOPHOS regional manager, Mr Jimi, outline the critical role cyber intelligence plays, amongst which are its ability to: Identify what threats exist in a system Understand threat propagating processes and scale of attacks Develop the right defense. The speaker thus summarized the uses of cyber intelligence to include; Identification of threats Risk assessment Policy formulation and framework building that give cyber resilience Fostering collaborations and awareness for holistic protection.	Ifeanyi Uche, Nigeria Police Force, National Cyber Crime Centre The speaker noted how the Nigeria National Cyber Crime Centre mandate of combating cybercrime and related offences. According to the speaker, intelligence sharing and analysis have been critical to the process of cyber security enhancement and cyber defense expansion. The police chief disclosed its role in dealing with several cyber threat actors, including an arrest of a major threat actor for executing about 600 transactions in 2 to 3 minutes.

5. Simulation Attack **Presentation.**

Mr Sam OKENYE, Chief Consultant, Bofem Consulting, presented a cyber attack simulation.

6. Raffle Draw and **Outcome.**

Based on the Leaderboard's rankings, the top five participants, ranked by points earned in the conference's raffle draw, each received a $100 Amazon gift card (*See Appendix ii*).

7. Closing **REMARKS.**

Closing remarks were delivered by Mr. Adeyinka SHONEKAN, Executive Director, CSCS.

8. **Conclusion.**

Technological evolution and intelligence like AI have become more integral to the functioning of all critical infrastructures, and recent years have seen security structures across the globe face evolving cyber risks and vulnerabilities. The evolving conditions demand stronger and more coordinated responses from all stakeholders. The CSCS 2024 conference, organized in partnership with the Office of the National Security Adviser (ONSA), is a strategic drive towards mitigating all forms of isolation effect by stakeholders in Nigeria's cybersecurity landscape. Conference participants emphasized the importance of fostering collaboration between public and private entities in investing in domestic solutions and critical information infrastructures. This collaboration is vital for leveraging AI opportunities to enhance growth, efficiency, and

trust within the economy and financial markets while underscoring the urgent need for proactive measures to combat cyber threats and attacks.

9. Key **Takeaways.**

- Technological innovations have become integrated and a key component of our daily lives.
  Technologies such as AI offer a duality of opportunities and threats.
- AI holds great promise; it must be complemented by the right infrastructure to harness its efficiencies and mitigate cyber risks.
- Security must be deeply integrated at every level in digital operations, especially in economies and markets where critical digital infrastructure is still developing.
- Protecting and securing critical information infrastructures will require investments through collaboration between all stakeholders.
- A whole-of-government and whole-of-society approach must be adopted.
- Protecting digital infrastructure has become paramount with the increased reliance on digital systems.
- Need for a continuous drive towards proactive IT-based solutions in heightening cybersecurity.
- There are significant risks to continuously running some of the Nigerian army's operational plans and procedures on foreign-based systems.
- Intelligence incorporation and collaborations must be heightened.
- Research and development activities must be invested in to understand the opportunities and threats emerging technologies continuously present.
- Skill gap remains a critical challenge to the cybersecurity landscape in Nigeria.

The Conference ended at **3.00 PM**

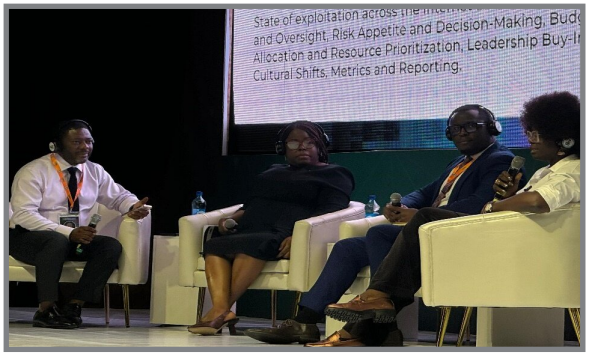
Rapporteur:
Terver AUDU, *Analyst, Proshare Nigeria*

For feedback and further information, kindly contact research@proshare.co

Appendix.

Appendix i: Panel Session and Discussants

Appendix ii: Raffle Draw leadership Board and Event Images:



Related **Items.**

1. CSCS Wins Capital Market Infrastructure Developer of the Year at BAFI Awards 2024.
2. Temi Popoola Calls for Unified Cybersecurity Strategies at CSCS Conference.
3. CSCS Strengthens Board with Appointment of Bola Adesola and Aisha Muhammed-Oyebode as Directors.
4. NGX Group GMD Elected CSCS Chairman.
5. CSCS Advocates FinTech innovation for Inclusive Capital Market.
6. BAFI 2023: CSCS Bags Digital Transformation and Cybersecurity Advocate of The Year Award.
7. NGX Working with CSCS, Euroclear to Create Dollar Settlement Platform for Fintechs.
8. FMDQ Holdings Plc Acquires 21.6% Stake in CSCS.
9. NGX Congratulates CSCS on 25th Anniversary, Urges Increased Synergies.
10. CSCS Set to Broaden Conversation on Cybersecurity in Nigeria.
11. CSCS Plc Joins ISSA's Board; Appoints CEO Haruna Jalo-Waziri as Board member.
12. CSCS Grows Revenue by 39.2%, Pays Shareholders Total Dividend of N3.7bn.
13. CSCS' Chief Executive, Jalo-Waziri, elected as Vice President of AMEDA.
14. FMDQ Group May Pay N20bn to Acquire 21.6% Stake in CSCS.
15. NGX Partners BUA Group, CSCS, and Other Private Sponsors to Host Capital Markets Conference.
16. CSCS Wins Depository, Custody Company of the Year Award.
17. CSCS Board Re-appoints Haruna Jalo-Waziri for Another 5-Year Term.
18. CSCS Bags Prestigious Market Choice Award for Enhanced Collaboration with Market Participants.
19. NSE CSCS joint Workshop for Capital Market Correspondents 301012.
20. 2021: CSCS Makes Commitment to Effective Collaboration for Market Stability.
21. CSCS Sensitizes Financial Market Stakeholders On The Value Of Cyber-Security.

22. CSCS Democratizes Issuance of ISIN, Becomes GLEIF Sole Operating Unit Based In Nigeria.
23. CSCS Will Leverage Technology To Attract Millennials Into The Capital Market - Haruna Jalo-Waziri.
24. Haruna Jalo-Waziri To Speak on CSCS Plc Activities Tomorrow On WebTV.
25. 26th CSCS AGM: Shareholders Approve N4.3bn Dividend, As Non-Core Revenue Grew 162.5% YOY.
26. CSCS To Hold 26th Annual General Meeting by Proxy On May 22, 2020.
27. COVID-19: CSCS Goes Fully Digital, Activates Business Continuity Plan.
28. CSCS Issues Statutory Fee Update Following Increase of VAT to 7.5%.
29. CSCS Launches Regconnect to Improve Market Service Delivery.
30. CSCS Holds 25th AGM, Pays Shareholders 70k Dividend.
31. CSCS PLC Records 12% Growth in Total Assets for 2018 FY.
32. Thomas Murray Upgrades CSCS To A Plus Outlook.
33. CSCS wins CFI.co Outstanding Contribution to the Capital Markets – Nigeria 2018 Award.
34. CSCS holds 24th AGM, pays shareholders 70k dividend.
35. NASD Introduces Trade Alert Notification Service; CSCS Holds 24th AGM.
36. Guide on CSCS Online Portfolio View Activation.

Advice To Users of This **Report.**

Proshare, founded in 2006, is a trusted professional practice and financial information hub dedicated to serving as a critical bridge between the markets, investors, regulators, and stakeholders. By delivering credible, reliable, and timely engagements, we assist the marketplace to shape thought-led conversations premised on evidence-based insights that hold the firm accountable collaboratively.

Practice Ethos and Disclaimer

Proshare does not guarantee any results or investment returns based on the information contained in this report. Although we have used our best efforts to provide the most accurate information, we do not promise verbally or in writing that you will earn a profit when or if you use the information contained therein and/or take the actions that might have been prescribed here by the author or our analysts, any reliance you place on our content for decision making is at your own risk Reports often contain complex technical language, kindly seek expert analysis or expert opinions to help interpret the findings accurately. Context is key, and understanding is essential to grasp the report's true implications. We encourage our discerning readers to seek additional education and insights as you navigate the complexities of the report. As consumers of news and information, we play a role in responsible reporting, be cautious of spreading unverified or misleading information about the report's contents or corporate entities mentioned in the report.

Creation Date

This report was published on December 04, 2024, and is based on the best publicly available information at that time. The PDF version was created on December 05, 2024. For comments, feedback, and updates, kindly send us an e-mail via **research@proshare.co**. Thank you.

Teslim **SHITTA-BEY**
Managing Editor/CE

Tosin **IGE**
Head, Research

Contacts.

Olufemi **AWOYEMI**, *mni*
ceo@proshare.co

Teslim **SHITTA-BEY**
teslim.bey@proshare.co

Tosin **IGE**
research@Proshare.co

Ademidun **SHOGO**
ireconomist@Proshare.co

www.proshare.co
+234 902 407 5284
@proshare
proshare.co
proshare.co
proshare.co

Plot 590b, Lekan Asuni
Close, Off Toyin Omotosho Street,
Omole Phase 2, Isheri Olowora
Ikeja, Lagos, Nigeria **PC: 105102**
Tel: **0700 – PROSHARE**
E-mail: info@proshare.co