KEYNOTE ADDRESS BY MR ADEKUNLE SONOLA, THE MD/CEO OF POLARIS BANK LIMITED AT THE 54TH QUARTERLY MEETING OF THE ASSOCIATION OF CHIEF AUDIT EXECUTIVES OF BANKS IN NIGERIA (ACAEBIN) ON THURSDAY DECEMBER 8, 2022

The Chairman, Association of Chief Audit Executives of Banks in Nigeria (ACAEBIN), Esteemed Members of ACAEBIN, Representatives of Regulatory Bodies, Other Stakeholders, Ladies and Gentlemen.

I wish to express my profound delight in welcoming you all to the quarterly meeting of the ACAEBIN. On behalf of the Management of Polaris Bank Limited, I wish to place on record my appreciation for the opportunity presented to our bank to host this meeting of your esteemed association. It is also gratifying to note the presence of representatives of other stakeholders such as the regulatory bodies and the law enforcement agencies.

The theme of this quarter's meeting tagged **"Cybersecurity threats & the challenges of building a sustainable financial sector: The way forward"** underscores the major threat affecting the banking industry today and the need for the CAEs to rise up to the challenge in discharging their responsibilities.

The Chief Audit Executives (CAEs) sit at a vantage position with oversight and assurance functions on IT, Information system security, Internal Control and other areas of the organization. It is therefore important for CAEs to continually evolve, learn, unlearn and relearn to meet the demand imposed by the adoption of technology for the overall protection of their organizations if they really want to remain relevant in the scheme of things.

Technology has evolved throughout human history and will continue to evolve into the future. In particular, computer technology has evolved so much within the last 100 years. From the time of mainframe computers and punch cards to the emergence of personal computers and the internet, the world is not looking back. This technological evolution has had so much impact on the way we do businesses especially banking business.

Today, most of our business and personal lives are rooted in our access to technology. From personal access to the web, alongside business platforms, third-party providers and apps, technology drives much of what we do on a daily basis. Practically, our lives is increasingly dependent on technology.

Information obtained from ***CompTIA*** revealed some interesting facts on how much technology has influenced our way of life which underscore the need for auditors to continually evolve:

1. The technology continue to grow at a steady rate, making information technology one of the fastest growing sectors in the world.
2. There are more than 5.1 billion active users on the internet as at 2022 while about 4.28 billion users access the web via mobile internet.
3. There are 4.2 billion active users on social media platforms.
4. ***Statista*** forecasts that emerging technologies will experience a growth rate of about 104% between 2018 and 2023.
5. Investments into IoT (Internet of Things) is expected to grow by nearly 14% in 2022 and ***Statista*** predicts that there will be 30.9 billion IoT devices by 2025.

A direct consequence of pervasive adoption of technology is the increase in sophistication and frequency of cyber incidents. Cyber threats are everywhere, and they are always changing. For many institutions, it could appear almost impossible to prepare for all threats, or to keep up to date with best practices in cybersecurity.

Cyber security risk is the real pandemic of modern times. It is ever present, increasing like a virus, and we cannot inoculate ourselves against it. The fact is that the increasing connectivity results in greater security risks, and hackings are becoming more frequent from a greater variety of actors. Let me share with you some interesting global statistics on cyber risks as reported by ***Cybersecurity Ventures***. These global statistics underscore the importance attached to cyber risks and the need for a holistic approach to handling them:

1. The imperative to protect the increasing digitized businesses, Internet of Things (IoT) devices, and consumers from cybercrime will propel global spending on cybersecurity products and services to an estimated $1.75 trillion cumulatively for the five-year period from 2021 to 2025, up from $1 trillion cumulatively from 2017 to 2021.
2. Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion by 2025, up from $3 trillion in 2015.
3. An amount of $20billion representing cyber security damages was attributed to ransomware in 2021, which is about 62X more than the $325 million reported in 2015.
4. Over an eight-year period tracked, the number of unfilled cybersecurity jobs grew by 350 percent, from 1 million positions in 2013 to 3.5 million in 2021.

Cyber security statistics shown above indicate that this field will only continue to grow commensurately with the demand for increased technological adoption. Hackers and cyber criminals aren’t slowing down and so, Chief Audit Executives

need to take a pragmatic approach to cyber security issues working with other relevant stakeholders.

With the increase in frequency and sophistication of cyber-attacks, the task of building a sustainable and resilient financial institution is becoming more challenging. From the high cost associated with maintaining an efficient cyber security program to the issue around attraction and retaining skilled technical resources, managers in financial services industry face hard choices.

To put cyber-threats in perspective, let us take a look at three broad categories of risks facing the financial services sector today:

People factor: At the top of the cyber threats that the financial services industry is facing is PEOPLE. If we talk about phishing attacks, people are the delivery medium. If we focus on malware, people are largely the execution factor, if we talk about weaknesses in systems configurations that allow an attacker to succeed in compromising systems, people are responsible for maintenance of such systems. If we take a look at insider related frauds and irregularities, we will see that people are at the centre of them all. The people factor remains a formidable threat agent for the survivor of any organization and its cyber resiliency. An emerging issues around people is the current high rate of staff attrition occasion mainly by "japa" syndrome and the attendant difficulty in resourcing to fill human capital vacancies.

Third Party Risk factor (Amplified by Open Banking): Another emerging threat factor that is beginning to influence the direction of cyber threat is third party risk. With increasing interconnectivity in the financial services sector and the growing global concept of Open Banking, this risk will increase exponentially in the coming years. Financial services currently rely heavily on the use of APIs to facilitate business-to-business connectivity. No matter how well protected an organization is, if a third party is weak, collectively the entire financial services industry will be weak because a chain is as strong as its weakest link.

Technology Risk factor: Technology and innovation are also a major risk factor for the financial services industry. The same cutting edge technologies (such as artificial intelligence and robotics) available to run businesses are also available to hackers and fraudsters and they are beginning to use them against organizations. In the coming years, we will experience more sophisticated attacks facilitated by cutting edge technologies and we need to be prepared for the challenge.

Ladies and gentlemen, from my perspectives, some of the following issues will aid our contribution to managing cyber security risks and their related threats to financial services:

1. The audit function can no longer remain analogue and gathering loads of files and documents to review transactions and events after the fact. To be

relevant and truly add value in this digital age, audit professionals must begin to build and acquire IT and digital skills. We have to move the audit function to the cutting edge of technology and begin to speak languages like machine learning, AI, cloud computing, IoT, as core levers of your trade. When technology solutions and applications are being conceived to meet operational or business needs in our institutions, the audit function must be actively involved in that process and ensure that audit capabilities are built into technology solutions in a manner that satisfies audit objectives.

2. Close the gap between audit and risk management functions while still maintaining the independence of internal audit function. Given the dictates of digital transformation, audit function must become more proactive and less reactive. The speed at which technology drives events, transactions etc and the associated scale of damage, require the auditors to become not only proactive but also online and real-time in delivery. This is where value lies and we must on-board every capability required including shift in mindsets, for us to discharge our duties effectively.

3. Collaboration – with the pace at which technology is changing the banking landscape, coupled with the interconnectedness of the financial system against the backdrop of open banking, audit partnership among financial institutions must lead the frontier of collaboration. Data gathering, information and knowledge sharing are few of practices we MUST begin to imbibe. We strengthen our adversaries and weaken our ability to check their nefarious activities if we chose to compete among ourselves than we collaborate for more audit effectiveness. I believe this is what ACAEBIN stands for and we must deepen engagements like this. Whilst we hone our strategies for collaboration at events like this, we must however take it beyond the hall of seminars and conferences into our daily operational activities.

4. Effective training of staff even up to the board level to continuously create necessary awareness around cyber security risks to enhance cyber resilience. When people are well trained, they can easily identify cyber threats and take steps to prevent cyber incidents.

5. Effective management of the current high rate of staff attrition in the technology related functions. Can we consider a recruitment pipeline for fresh graduates to take positions under the supervision of experienced hands. Another approach is to consider formulating remote work policies and a way of retaining the services of very experience hands who may be willing

to continue rendering services to the organization under a remote work arrangement.

6. Effective management of third party risks by a combination of the following measures:
    - Having a strong service level agreement/contract with third parties
    - Conducting regular onsite/offsite assessment of the third parties to ensure they have or maintain minimum security standards
    - Conducting cyber-security awareness training for third parties based on the risk assessment you have conducted on them
    - Deploying relevant technologies to protect the connections you may have established with third parties

7. Effective management of technology risk through the constant investment in technologies. Modern cyber security program rely heavily on cutting edge technologies such as artificial intelligence (AI), Robotics and others. Furthermore, cyber risk is constantly changing and evolving, security solutions implemented in the past may have become obsolete and in-capable of handling current threats. It is therefore necessary for you as auditors to continue to draw the attention of your Management towards sustaining investment in cyber security solutions for the protection of our information assets.

Conclusion

So, as you deliberate during the session today, I sincerely request that you explore ways by which the overall cyber security risks in the financial services industry can be effectively managed. I urge you to pay particular attention to the issues of skill gaps, information sharing, and effective engagements with law enforcement agencies and regulators on speedy conclusion of investigations, apprehension of suspects and prosecution of those found culpable.

I thank you all for listening and i wish you a happy Xmas and a prosperous year 2023.

Thank you.