OFFICIAL LAUNCH OF NATIONAL CYBER SECURITY AWARENESS MONTH(NCSAM) 2021

A DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE(CII) AND THE CYBER SECURITY AUTHORITY(CSA)

POLICY DIRECTIVE SPEECH

BY

DR. MAXWELL OPOKU-AFARI

FIRST DEPUTY GOVERNOR, BANK OF GHANA

NCA CONFERENCE ROOM

OCTOBER 1, 2021

Minister for Communications & Digitalisation

Minister for Energy

Selected Members of Parliament

Former Ministers of State

The US Ambassador,

The Director-General of the National Communications Authority

Ag. Director-General of the Cyber Security Authority

CEOs from the Critical information Infrastructure Sectors including from the Telcos & Banks

Members of the National Cyber Security Technical Working Group (NCSTWG)

Distinguished Guests, Ladies and Gentlemen

Good morning and as always, it is a great pleasure to be here today to be discussing issues of cybersecurity which has gained heightened attention in recent times. Before I begin, let me commend the organizers of this programme for their thoughtfulness and for bringing together players in the cyber security space to share experiences on all these important issues, and it is my fervent hope the issues discussed and lessons learnt would strengthen our resolve to counter cyber threats in the economy.

Let me also thank the National Cyber Security Centre for extending an invitation to me to speak to such a distinguished audience on such an important issue which has become top priority amongst most governments and private sector institutions, not here alone in Ghana but across the globe. It is also important to me because it also affords me to share with participants the steps being taken at the Central Bank to protect the financial sector from

cybersecurity threats and related activities. This is important to assure the banking community of our efforts to safeguard the banking system and put it on that steady pedestal towards supporting growth. It is indeed an honour to be able to join you today.

The gradual evolution and change in the business models of firms and institutions and the speed with which the entire digitalization agenda is progressing is forcing us to re-think ways and means of protecting the very infrastructure that supports this new way of life. Analysts have predicted that the next financial shock or shock to the global economy could manifest itself in the form of a cyber-attack and this makes it imperative for us to begin to think of how to secure and protect our infrastructure

Cyber-attacks (i.e. attacks on information and communication technology systems) have emerged as a global threat to financial stability and our way of life. Successful cyber-attacks on computer systems and networks supporting critical national assets and infrastructure could cause significant havoc to our way of life, cause financial loss, undermine public confidence, and cause major disruption to our economy. I am therefore encouraged that all the major stakeholders are gathered here today to launch a national effort aimed at creating cyber security awareness to combat the rising threat posed by cyber-attacks and cyber-crimes. It is my hope that the steps we are taking today will be sustained to promote confidence in the financial system and also ensure financial inclusion.

Mr Chairman, let me also add that the COVID-19 pandemic, and issues emanating from it, has accelerated the adoption of digitalization in Ghana and this is progressing at top speed. Embracing the new norm of working remotely, transferring resources across financial platforms, purchasing goods and services online e.t.c., are gradually changing the face of our

economy and we need to position ourselves in readiness for the threats that come along with this changing lifestyles and doing business. The pandemic has also impacted cybersecurity in various ways, including:

- Bringing to the fore a rapidly evolving cybersecurity threat landscape that has rendered traditional or conventional cybersecurity safeguards inadequate; and
- Increased cybersecurity exposure for Critical Information Infrastructure.

These new and emerging threats have left nations and organizations exposed and vulnerable to cyber-attacks. Current trends in cybersecurity point to significant increases in attacks against Critical Information Infrastructure and related organizations that are drivers of national economies. For many organizations today, the concern is no longer "**if or when the organization is hacked**", but rather "**the organization is likely hacked, we just don't know how and when it happened**".

Addressing cyber security risks has become more important than ever and policy makers need to internalize this fact in their discourse. In what follows, I will discuss regulatory regimes that are being followed through to enhance cybersecurity awareness in the banking sector. We are all aware that the banking sector is one critical institution whose role is to support growth. Over the years, banks have progressively moved to digitize their operations and in the process have become vulnerable to cyberattacks. Our inability to put in place policies to protect the infrastructure of banks from attacks could result in the destruction of the very foundation of growth and this has national security implications. Regulating and close monitoring of cyber activities in the banking sector thus become an important critical role for the central bank. While we pursue this agenda, we need to recognize that regulatory

frameworks alone may not be enough to protect the nation's critical information infrastructure. Regulatory frameworks must be followed by actionable steps to lock-in potential intentions. For this reason, I will attempt to go through some issues and highlight the importance of cyber security awareness including on cyber hygiene as a means of confronting head-on cyber security risks.

Globally, cyber-attacks on digitized payment products are increasingly becoming sophisticated, especially on financial institutions with insecure IT systems. We have witnessed global cyber-attacks which resulted in disruptions to some critical financial services and destroyed financial assets and savings. It is important therefore to ensure that the security of electronic banking products and services are not compromised.

National Response and Preparedness

At the National level, the Government of Ghana recognizes the threat cyber-attacks and cybercrimes poses to critical information infrastructure as well as the damage it can cause to the trust and confidence in our financial system. As a result, the Government responded swiftly through regulatory measures such as the Data Protection Act, 2012 (Act 843) and the Cybersecurity Act, 2020 (Act 1038), as well as supporting directives and other related legislation to enforce provisions of the law across all sectors of the economy.

The Data Protection Act, 2012 (Act 843) recognizes a person's right to protect and safeguard their personal data and the Act sets out eight (8) basic principles for those institutions who control data to implement

measures to protect the rights of data subjects and safeguard their personal information.

At the same time, the new Cybersecurity Act, 2020 (Act 1038): makes provision for the protection of Critical Information Infrastructures in the country including information under the control of the financial sector which is identified as a prime sector. Section 44 of the Cybersecurity Act, 2020 (Act 1038) further provides the legal basis for BoG to lead the Sectoral Computer Emergency Response Team (CERT) for the financial sector, and I must say that as far as this is concerned work has already started to ensure the deployment of a security setup that provides real-time visibility into cyber threats and attacks targeting the financial sector.

Mr Chairman, Given the increasing spate of cyber-attacks on the Financial sector worldwide, which has become more frequent with sophistication in recent times, and given the fact that our financial sector has also had its fair share of these attacks, The Bank of Ghana, as far back as October 2018 took actionable steps to issue the Cyber and Information Security Directive in a bid to enhance and protect the security of this critical sector of our economy.

The Directive, at the time was aimed at creating a secure environment within the cyberspace for the financial services industry and thus serve to generate adequate trust and confidence in Information Communication and Technology (ICT) systems. Following the issuance of the Directive, the Bank of Ghana has introduced many initiatives to strengthen and secure the information security architecture of the banks, to ensure the systems at the banks are robust and resilient.

Mr Chairman, permit me at this stage to list a few of the actions we have taken in this regard:

a. The Bank of Ghana has worked collaboratively with the commercial banks to meet the governance requirements of the Directive, that is, appointments of Board Committee on Cyber and Information Security with a clear Charter; assignment of Director of Cyber and Information Security (DCIS); and appointment of Chief Information Security Officers (CISOs).

b. Banks have been reporting their cyber and information security incidents to the Bank of Ghana on monthly basis.

c. The Bank of Ghana continues to have periodic engagement with member banks to clarify aspects of the Directive.

d. The Bank of Ghana, through the Directive, has facilitated safer digital transformation with the adoption of cloud technologies.

e. So far, the Bank of Ghana has prepared a banking sector Cyber and Information Security guidelines to protect consumers and create a safer environment for online and e-payments products. Among others, the guidelines seek to create a secure environment for transactions within the cyberspace and guarantee trust and confidence in ICT systems; provide an assurance framework for the design of security policies in compliance to global security standards and best practices by way of cyber and information security assessments, and protect banks, customers and clients against the potentially devastating consequences of cyber-attacks.

In pursuing these objectives, the Bank of Ghana has embarked on the Financial Industry Command Security Operations Center (FICSOC)

project to enable the industry have aggregated visibility into the cyber threat landscape confronting the sector, through monitoring and threat intelligence sharing. The components of the FICSOC Project include:

1. **Security Information and Event Management (SIEM):** With the SIEM, a collector will be placed at each member bank's premises to collect security alert streams from the banks and forward them to the FICSOC over a dedicated secured network for monitoring, analysis and information sharing.
2. **Threat Intelligence Sharing:** Regarding the sharing of intelligence threat, threat intelligence nodes will be placed at each member bank's premises to receive relevant threat intelligence, including Indicators of Compromise (IoCs) from the FICSOC.
3. **Network Traffic Analysis:** Network traffic analysis is an important component of the FICSOC at each member bank that inspects Internet traffic for malicious or suspicious content and sends constant reports to the FICSOC for analysis.
4. **Digital Forensic Laboratory:** The FICSOC Project will also provide a Digital Forensics Laboratory comprising digital forensic evidence collection and storage facility, evidence processing rooms, and spaces for Examiners to discuss cases and hold relevant briefing.

Not all these can be possible without the requisite human capacity needs, and Bank of Ghana is looking into these issues closely to ensure sound implementation and rollout of these objectives. A cybersecurity expert with appropriate digital forensics capability will support the BOG in these efforts to help fully deploy the project.

It is anticipated that this integrated approach to cyber security management would support financial institutions achieve both business and security focused objectives, as well as regulatory compliance in an efficient and effective way.

Mr. Chairman, regulatory compliance by itself is not cyber security. The onus lies on banks to examine the state of their security systems, identify gaps and design appropriate mechanisms to counter possible cyber threats. In addition to these cyber security regulations, financial institutions will also be required to implement an integrated approach by adopting enterprise-wide frameworks of cyber risk management in line with business objectives.

Mr. Chairman, a lot has been said already in this forum on Cybersecurity Awareness and the role of employees in combating cyber-attacks, cyber-security training, and the need to have in place a cyber-security hygiene policy. I don't intend to re-hash these issues again but I believe as institutions strive to make their workplaces more cyber-safe, these critical elements discussed in detail will form part of future policy design.

The Way Forward

Today's world is completely different from a decade ago as changes in information and communication technology increase exponentially. As a result, it is important for institutions to undertake cyber security-related due diligence and assessments, identify proper detective controls, and enforce third party and insider risk programmes to protect and safeguard their working environments from cyber related activities that are not conducive for growth. I believe we will all delve into some of these critical issues that are associated with our drive towards digitization.

We at the Central bank will continue to draw strength from Act 1038, which is intended to further promote and improve collaborative efforts between the Cyber Security Authority and the Bank of Ghana. The Central Bank will work closely with the Cyber Security Authority to monitor trends of cybersecurity issues in the financial sector and ensure collaborative response to cybersecurity incidents. The Bank of Ghana will also play an active role in the implementation of the Cybersecurity Act, 2020 through our representation on the Joint Cybersecurity Committee (JCC) pursuant to Section 13 of Act 1038. We will endeavour to provide all support available to ensure smooth formulation of policies in this area.

On the basis of these, I wish you all fruitful deliberations.

Thank You for your kind Attention.