MINISTRY OF COMMUNICATIONS & DIGITALISATION

CYBER SECURITY AUTHORITY CSA

NATIONAL CYBER SECURITY AWARENESS MONTH 2022

REPORT



REGULATING CYBERSECURITY

A Public - Private Sector Collaborative Approach



CYBER SECURITY AUTHORITY (CSA)

A SECURE AND RESILIENT DIGITAL GHANA



Cooperation is Key

Contents

i Acknowledgements

ii Acronyms

iii Executive summary

v National Cybersecurity Leadership

vi Overview of the Cybersecurity Act

viii Institutional Framework

x Governing Board of the CSA

xi Joint Cybersecurity Committee

xii Overview of the CSA

01 Media Launch Of The National Cyber Security Awareness Month (NCSAM) 2022 Edition

06 Launch Of The Cyber Security Awareness Month For Members Of The Ghana Armed Forces

Week 1 Cybersecurity Industry Focus

10 Official Launch of NCSAM 2022- Regulating Cybersecurity: A Public-Private Sector Collaborative Approach

16 Public Consultation on Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals.

21 Forum on Ghana's Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals

Contents

Week 2 — Computer Emergency Response Team(CERT) / Critical Information Infrastructure Protection (CIIP) Focus

26 Public Consultation on Framework for Accreditation of Sectoral CERTs

31 Compliance Workshop on the Directive for the Protection of Critical Information Infrastructure

Week 3 — Child Online Protection (COP) / Civil Society Focus

36 National Cybersecurity Challenge for Senior High Schools

41 Civil Society Forum on Cybersecurity Regulations through Strategic Partnership

46 Breakfast Meeting on "Ghana's Cybersecurity Act, 2020 (Act 1038); the Bank of Ghana Cyber and Information Security Directive; Its Implications and the Role of Board of Directors"

52 Technical Training for Personnel of the CSA and Other Joint Cybersecurity Committee Institutions

56 Stakeholder-Related Events

63 International Cooperation Related Events

80 Media Engagements

83 Conclusion

84 Recommendations

87 Photo Gallery

110 Partners & Sponsors

Acknowledgements

The theme for the 2022 edition of the National Cyber Security Awareness Month (NCSAM) was ***"Regulating Cybersecurity: A Public-Private Sector Collaborative Approach".*** I must say we have had successful collaborations with all key stakeholders and are hopeful that these collaborative efforts will yield positive outcomes that will ensure the security of Ghana's cyberspace.

The Cyber Security Authority (CSA) is grateful to His Excellency, the Vice President, H.E Dr. Alhaji Mahamudu Bawumia, and his representative, the Minister for Public Enterprises, Hon. Joseph Cudjoe, for the keynote speech and launch of the month-long event; the Minister for Communications and Digitalisation, Hon. Mrs. Ursula Owusu-Ekuful, whose impeccable leadership has contributed to Ghana's level of cybersecurity development and her able Deputy Minister, Hon. Ama Pomaa Boateng, who Co-Chaired the Steering Committee and gave high-level remarks at most of the events. We also acknowledge Hon. Albert Kan Dapaah, Minister for National Security and Hon. Kojo Oppong Nkrumah, Minister for Information, for the support they gave to the event.

Further commendation goes to the members of the CSA Governing Board and the members of the Joint Cybersecurity Committee for their continuous direction and involvement in the NCSAM programmes. The Authority is grateful to the CEO of the Rwandan National Cyber Security Authority, Colonel David Kanamugire, and Board Chairman of the National Information and Communications Technology Institute of Mozambique, Prof. Lourino Alberto Chemane, who came to Ghana with their respective delegations and signed Memoranda of Understanding with the Authority for future collaborations in cybersecurity development. We thank the members of the Diplomatic Corps, Heads of Security and State Institutions, CEOs from private sector institutions, representatives from Civil Society Organisations, Industry players, our partners and sponsors, the media and all who were involved in different ways to build capacity and to create awareness for a ***Safer Digital Ghana***. An expression of gratitude is also extended to the Steering Committee and the various sub-committees and the staff of the CSA for the excellent work done in organising the National Cyber Security Awareness Month (NCSAM) 2022.



DR. ALBERT ANTWI-BOASIAKO
Ag. Director-General, Cyber Security Authority

Acronyms

AfCFTA	African Continental Free Trade Area
BOST	Bulk Oil Storage and Transportation Company Limited
CBAC	Capacity Building and Awareness Creation
CCPE	Council of European Prosecutors
CERTs	Computer Emergency Response Teams
CEs	Cybersecurity Establishments
CID	Criminal Investigations Department
CII	Critical Information Infrastructure
CoE	Council of Europe
COP	Child Online Protection
CPs	Cybersecurity Professionals
CSA	Cyber Security Authority
CSOs	Civil Society Organisations
CSPs	Cybersecurity Service Providers
CVE	Countering Violent Extremism
DPC	Data Protection Commission
ECG	Electricity Company of Ghana
ECOWAS	Economic Community of West African States
EJCN	European Judicial Cybercrime Network
EOCO	Economic and Organised Crime Office
GAF	Ghana Armed Forces
GBA	Ghana Bar Association
GIFCT	Global Internet Forum to Counter Terrorism
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GJA	Ghana Journalists' Association
GNAT	Ghana National Association of Teachers
GNCCI	Ghana National Chamber of Commerce and Industry
GWCL	Ghana Water Company Limited
ICT	Information and Communications Technology
ISACA	Information Systems Audit and Control Association
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
ICT	Information and Communications Technology
ISACA	Information Systems Audit and Control Association
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
JCC	Joint Cybersecurity Committee
KAIPTC	Kofi Annan International Peacekeeping and Training Centre
MLA	Mutual Legal Assistance
MoCD	Ministry of Communications and Digitalisation
NCC	National Cybersecurity Challenge
NCPS	Ghana's National Cybersecurity Policy and Strategy
NCSAM	National Cyber Security Awareness Month
NIB	National Intelligence Bureau
NITA	National Information Technology Agency
NITA-SOC	National Information Technology Agency- Security Operations Centre
NPA	National Petroleum Authority
NSB	National Signals Bureau
PPP	Public Private Partnerships
SOC	Security Operations Centre
SOEs	State-Owned Enterprises
TaT	Tech Against Terrorism
TCAP	Terrorist Content Analytics Platform
UNCAC	United Nations Convention against Corruption Consultative
UNICEF	United Nations International Children's Emergency Fund
UPSA	University of Professional Studies, Accra

Executive Summary

Ghana is ranked 3rd on the African continent with a rating of 86.69% by International Telecommunication Union's (ITU) Global Cybersecurity Index report, 2020 – an improvement from the 10th (32.6%) and 11th (43.7%) positions in 2017 and 2018 respectively. The index measures cybersecurity efforts around five pillars to produce an aggregated score. These pillars are Legal, Technical, Organisational, Capacity Development and Cooperation Measures. Ghana's legal and technical measures were projected as areas of relative strength mainly owed to the introduction of the landmark Cybersecurity Act, 2020 (Act 1038). The areas highlighted for potential growth were Capacity Development and Cooperative Measures. By indication, the country's cybersecurity profile is built on these strong foundational pillars. However, the implementation of priority and strategic measures such as regulatory interventions through effective collaboration and partnerships are imperative for the improvement of the areas highlighted by the index.

The Cybersecurity Act, 2020 (Act 1038) provides the legal basis for the implementation of high-priority regulations by the Cyber Security Authority (CSA) to address the concerns raised by the index. These regulatory interventions are focused on Critical Information Infrastructure Protection (CIIP) (Sections 35-40); Computer Emergency Response Team (CERT) Development (Section 41-46) involving Sectoral CERT Accreditation and Information Sharing procedures; Licensing of Cybersecurity Service Providers (Section 49-56); Accreditation and Certification of Cybersecurity Professionals and Practitioners (Section 57-58); Cybersecurity Standards and Enforcement (Section 59); and Service Provider Retention of Data (Section 77), among others. The CSA has prioritised actions for the implementation of these interventions via collaboration and partnership efforts. In addition, Act 1038 emphasises on the need for effective collaboration and partnerships to promote public and private sector stakeholders' involvement in the country's cybersecurity development under Sections 13 and 81. Section 13 provides for the establishment of a Joint Cybersecurity Committee (JCC) consisting of heads of public sector institutions with a mandate on cybercrime/cybersecurity matters to collaborate to implement relevant cybersecurity measures. The JCC has been inaugurated to this effect. Furthermore, pursuant to Section 81, an Industry Forum is to be established to provide a platform for industry players from the private sector to periodically come together to discuss matters of common interest to the industry.

As part of measures to effectively implement Act 1038, the CSA sought to leverage on the 2022 edition of the annual National Cyber Security Awareness Month (NCSAM) to build synergy among public-private sector stakeholders for collaboration and partnerships to implement the key cybersecurity regulations and to build capacity among critical stakeholders. There was also the need to build upon cybersecurity awareness creation efforts through the implementation of the Safer Digital Ghana campaign. Following consultations with stakeholders, the Cyber Security Authority (CSA) adopted 'Regulating Cybersecurity: A Public-Private Sector Collaborative Approach' as the theme, highlighting the need for public-private collaboration in regulating cybersecurity in the country.

The month-long event focused on key priority areas, consistent with the programme of activities of the Authority and these were:

i. Regulations and Protection of Critical Information Infrastructure (CII).
ii. Regulations of Cybersecurity Service Providers and Cybersecurity Professionals.
iii. Accreditation of Sectoral Computer Emergency Response Teams (CERTs).
iv. Regulations and the Implementation of Investigatory Powers in Act 1038.
v. Regulations and the Protection of Children Online.
vi. Joint Initiatives/Programmes (CSA with JCC members and private sector, international partners, etc.)
vii. International Cooperation – (MoU with Rwanda, Mozambique, etc.)
viii. Stakeholder/partnership events and activities.
ix. Traditional and social media activities, etc.

The following key events were organised to achieve the objectives of the NCSAM:

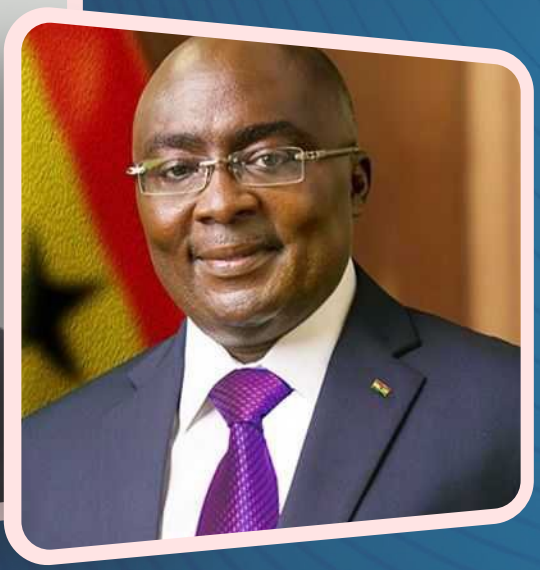
i. Media Launch of NCSAM 2022
ii. Launch of Cybersecurity Awareness Programme for the Ghana Armed Forces as part of NCSAM 2022
iii. Public Consultation on Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals and Practitioners
iv. Forum on Ghana's Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals
v. Public Consultation on Framework for the Accreditation of Sectoral CERTs
vi. Compliance Workshop on the Directive for the Protection of Critical Information Infrastructure
vii. National Cybersecurity Challenge for Senior High Schools
viii. Civil Society Forum on Regulating Cybersecurity through Strategic Partnership
ix. Cyber Security Authority / Ghana Association of Banks, Bank Boards and Executive Directors Briefing on "Ghana's Cybersecurity Act, 2020 (Act 1038); The Bank of Ghana Cyber and Information Security Directive; Its Implications and the Role of Board of Directors"
x. Technical Training on Cybersecurity for Selected Staff of the Cyber Security Authority and Joint Cybersecurity Committee Institutions.

To conclude, the events were successfully organised as scheduled and it is worth acknowledging that a number of civil society groups and societies organised awareness programmes for their constituents and these were augmented by high-level media engagements in some selected regions in the country.

National Cybersecurity Leadership



H.E. NANA ADDO DANKWA AKUFO-ADDO
President of the Republic of Ghana



H. E. ALHAJI DR. MAHAMUDU BAWUMIA
Vice President of the Republic of Ghana



HON. MRS. URSULA OWUSU-EKUFUL
Minister for Communications and Digitalisation



HON. AMA POMAA BOATENG
Deputy Minister for Communications and Digitalisation



DR. ALBERT ANTWI-BOASIAKO
Ag. Director-General, Cyber Security Authority

Overview of the Cybersecurity

Section 2- 4

Cyber Security Authority

Section 5-28

Governance of the Authority, Administrative & Financial Provisions

Section 29-34

Cybersecurity Fund



Section 47-48

Cybersecurity Incident Reporting

Section 49-56

Licensing of Cybersecurity Service Providers



Section 62-68

Protection of Children Online and other Online Sexual offences

Section 69-77

Cybersecurity and Investigatory Powers



Act, 2020 (Act 1038)



Institutional Framework



Non-Government Representatives

- → Private Sector
- → Business
- → Civil Society Organisations
- → Academia
- → International Partners / Organisations
- → Professional / Industry Associations

Governing Board of the Cyber Security Authority



HON. MRS. URSULA OWUSU-EKUFUL
Minister for Communications and Digitalisation (Chairperson)



HON. ALBERT KAN-DAPAAH
Minister for National Security



HON. AMBROSE DERY
Minister for the Interior



HON. DOMINIC NITIWUL
Minister for Defence



DR. ALBERT ANTWI-BOASIAKO
Ag. Director-General, Cyber Security Authority



AMB. ESTHER DZIFA OFORI
President's Representative



MRS. MAVIS VIJAYA AFAKOR AMOA
President's Representative



MRS. ADELAIDE BENNEH-PREMPEH
President's Representative



PROF. BOATENG ONWONA-AGYEMAN
Industry Forum



MR. CARL A. SACKEY
Industry Forum



MR. REGINALD BOTCHWEY
Industry Forum

Members of the Joint Cybersecurity Committee



DR. ALBERT ANTWI-BOASIAKO
Ag. Director-General, CSA



JUSTICE AFIA SERWAH ASARE-BOTWE
Superior Court of Judicature



MR. RICHARD OKYERE-FOSU
Director-General, NITA



MR. JOE ANOKYE
Director-General, NCA



MS. PATRICIA ADUSEI-POKU
Executive Director, DPC



DR. MAXWELL OPOKU-AFARI
1st Deputy Governor, BoG



MR. KWAKU DUA
Chief Executive Officer, FIC



NANA ATTOBRAH QUAICOE
Ag. Director-General, NIB



COP. MAAME YAA TIWAA ADDO-DANQUAH
Executive Director, EOCO



DCOP. MR. FREDERICK AGYEI
Deputy Director-General, CID



COL. (DR) TIM BA-TAA-BANAH
Director, NCTFC



MR. KWABENA ADU-BOAHENE
Director-General, NSB



MAJ. GEN. A. Y. NSIAH
Chief of Defence Intelligence, DI



MR. LAUD AKWASI AFFRIFAH
Deputy Comptroller-General, GIS



AMB. GEORGE ABAKA BLANKSON
Deputy Director-General, RD



COL. A. K. ODUAH
Ag. Director-General (DCIS), GAF



MS. YVONNE ATAKORA OBUOBISA
Director of Public Prosecutions



MR. NANA KOFI ASAFU-AIDOO
Executive Director, GDNR

Overview of the CSA

The Cyber Security Authority (CSA) has been established by the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country and to provide for related matters.

The CSA officially started operations on October 1, 2021; starting as the National Cyber Security Secretariat (NCSS) with the appointment of the National Cybersecurity Advisor in 2017 and later transitioned into the National Cyber Security Centre (NCSC) in 2018 as an agency under the then Ministry of Communications.

Core Values



Confidentiality



Inclusiveness



Integrity



Commitment



Reliability



Professionalism



Mission

To Build a Resilient Digital Ecosystem; Secure Digital Infrastructure; Develop National Capacity; Deter Cybercrime; and Strengthen Cybersecurity Cooperation.



Vision

To ensure a Secure and Resilient Digital Ghana.

Mandate of the CSA



Media Launch Of National Cyber Security Awareness Month (NCSAM) 2022 Edition

NATIONAL
CYBER SECURITY
AWARENESS MONTH

MEDIA LAUNCH OF NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2022 EDITION



Background

To achieve the goal of the 2022 Edition of the National Cyber Security Awareness Month (NCSAM), which is to promote public-private sector collaboration and partnerships on cybersecurity regulations, the month's events were preceded by a Media Launch on September 14, 2022 at the Press Centre of the Ministry of Information. The event was to create awareness for NCSAM 2022 and to call on Government-sector institutions, businesses and the general public to get involved in the celebration.



Opening Remarks

Hon. Fatima Abubakar
Deputy Minister for Information

Hon. Fatima Abubakar who moderated the event, welcomed everyone to the press briefing and indicated that the event was very important to ensure that all Ghanaians got involved in the National Cyber Security Awareness Month. She added that awareness creation was critical to ensure that everyone who used the internet gained optimum benefit.



Welcome Address

Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation

Hon. Ama Pomaa Boateng welcomed all dignitaries present especially personnel from the Media and stated her excitement to be present at the media Launch of the forthcoming NCSAM.

She indicated that Government is desirous to accelerate inclusive growth through greater efficiency, transparency, and accountability in the delivery of public services which has led to the implementation of various digitalisation projects. She however expressed concern about the increase in cyber-related incidents and crimes due to the over-reliance on Information Communications Technology (ICT) for socio-economic activities.

She stressed that cybersecurity is key to sustaining Ghana's digitalisation agenda and hence the need to have effective measures "to protect our critical information infrastructure, coordinate and respond to cybersecurity incidents, and to develop a cybersecurity culture in the interest of our socio-economic development". She added that Government was committed to its mandate as an enabler in the development of cybersecurity in the country and called on all Ghanaians to collectively take responsibility for the protection of the digital ecosystem.

Presentation

Dr. Albert Antwi-Boasiako
Ag. Director General, CSA



Dr. Albert Antwi-Boasiako began his presentation with statistics which indicated that the proliferating use of the internet has increased online vulnerabilities and opened more room for criminal activities. He noted that "in recent years, there has been several major cyber incidents that have significantly impacted businesses including financial institutions and other critical information infrastructure worldwide. That is to say, as dependency on digital technologies surge, so does cybercrime. Cybercriminals are seizing every opportunity to exploit vulnerabilities against people, businesses and organisations; having a grave impact on the confidentiality, integrity, and

availability of systems and networks, including critical information infrastructure".

Giving a history of Ghana's awareness month celebrations, he recalled that in January 2018 under the leadership of Hon. Mrs. Ursula Owusu-Ekuful, a cybersecurity maturity assessment was commissioned and conducted by the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford in collaboration with the World Bank. The assessment rated Ghana's cyber culture and society as the most serious area of concern to bridge the knowledge and awareness gaps of citizens on cybersecurity/cybercrime and related matters. This development, he said, led to the policy decision to formally institutionalise the country's cybersecurity awareness creation efforts in 2018, extending it from a week to a month-long programme consistent with best practices.

Focusing on the theme for this year's celebration, ***Regulating Cybersecurity: A Public-Private Sector Collaborative Approach***, Dr. Antwi-Boasiako, said globally, regulatory compliance has become one of the most effective and reliable strategies to mitigate cyber risks within the industry and that, "the implementation of cybersecurity regulations is imperative to deal with both existing and emerging cyber threats which have the potential to undermine the digital dividends expected from our digital economy".

He reiterated that the focus of NCSAM 2022, was to engage with stakeholders for inputs into the various regulations which are expected to take full effect starting January 2023.

He urged all stakeholders to participate fully in the events for an effective outcome whilst calling on the private sector, churches, schools, Civil Society Organisations, the media and the entire public to use the period to educate their members or constituents on cybersecurity.


Dr. Ing. Kenneth Ashigbey
CEO, Ghana Chamber of Telecommunication

Remarks

Dr. Ing. Kenneth Ashigbey
CEO, Ghana Chamber of Telecommunication

Dr. Ing. Kenneth Ashigbey, Chief Executive Officer of the Ghana Chamber of Telecommunications stated that the development of cybersecurity requires a collaborative approach, therefore urged the telecommunications sector to take cybersecurity issues seriously and to work with their clients to reduce the rate of mobile money scams and fraud. He encouraged academia, the private and public sectors, and Civil Society Organisations (CSOs) to raise cybersecurity awareness among stakeholders.

Remarks

Mr. Daniel Gyampo
President, ISACA (Accra Chapter)

The President of the Information Systems Audit and Control Association (ISACA), Accra Chapter, Mr. Daniel Gyampo, remarked that the awareness month was significant since it had the potential to draw investment into the country. "A good perception of cybersecurity is now as good as capital because more enterprises will start to move in when international business people regard Ghana as a safe environment," he said.



Mr. Daniel Gyampo
President, ISACA (Accra Chapter)

He encouraged Ghanaians to incorporate cybersecurity into their everyday lives, whilst suggesting that cybersecurity education should begin in the primary grades to help develop a culture of cybersecurity in the country. Mr. Gyampo called on senior managements to be guided by compliance frameworks, enforcements, and standards to ensure the safety of IT systems in critical areas of the economy.

Remarks

Major-General Dr. Emmanuel Kotia
CEO, Ghana Boundary Commission



Major-General Dr. Emmanuel Kotia
CEO, Ghana Boundary Commission

Major-General Dr. Emmanuel Kotia, Chief Executive Officer of Ghana Boundary Commission, emphasised that to create a robust cyber ecosystem, "we must first understand and abide by the provisions in the Cybersecurity Act, 2020 (Act 1038)". He stressed that cybersecurity is a national and developmental issue and hence the need for all stakeholders to collaborate in its development.



Conclusion

In closing, Honourable Fatimatu Abubakar, Deputy Minister for Information, urged the media to become ambassadors of cybersecurity in Ghana.

Launch Of The Cyber Security Awareness Month For Members Of The Ghana Armed Forces

NATIONAL
CYBER SECURITY
AWARENESS MONTH

LAUNCH OF THE CYBER SECURITY AWARENESS MONTH FOR MEMBERS OF THE GHANA ARMED FORCES



Background

Cybersecurity has become essential in this digital age as such, it's activities and implication on national security cannot be overlooked. The repercussions of cybersecurity issues on various organisations have made it imperative to all stakeholders. In line with the National Cyber Security Awareness Month, the Ghana Armed Forces organised awareness month programmes for its members and this was preceded by a media launch on September 30, 2022 to create awareness on the need to secure the Ghana Armed Forces Digital ecosystem which includes education on good cyber hygiene and best practices amongst others.

Remarks

Colonel A. K. Oduah
Ag. Director-General, Defence Communications and Information Systems of the Ghana Armed Forces

Col. Oduah stated that the world has become interconnected through supercomputers and massive network systems as well as the internet which has been the components for the development of the cyberspace. He said cybersecurity awareness has become very important in an age where many computers connected to the internet are becoming



Colonel A. K. Oduah
Ag. Director-General, Defence Communications and Information Systems of the Ghana Armed Forces

vulnerable and exposed to threat actors such as viruses and malware. Colonel Oduah stated that it was important for the Ghana Armed Forces to leverage on the National Cyber Security Awareness Month 2022 to intensify its capacity building and awareness creation efforts on cybercrime while educating all military ranks on the importance of cyber hygiene to create a better understanding of the vulnerabilities in the digital ecosystem.

Remarks

Col. Z Ayorrogo
Provost Marshal

Col. Ayorrogo's remarks focused on cybersecurity incidents and their impact on the Ghana Armed Forces. He stated that cybersecurity fraud has been the most reported incident over the past 5 years in the Ghana Armed Forces and the recorded cyber fraud cases were connected to recruitment where



images of service commanders of the Ghana Armed Forces and Chief of Defence Staff were used for advertisement by cyber fraudsters for impersonation and extortion on various social media platforms. He urged the media to support the Ghana Armed Forces and the Cyber Security Authority to increase awareness creation to the public on cybersecurity matters.

Remarks

Dr. Albert Antwi-Boasiako
Ag. Director General, CSA

Dr. Albert Antwi-Boasiako commended the Ghana Armed Forces (GAF) for the invitation and for efforts to improve cybersecurity in the GAF. He cited the GAF as the first Joint Cybersecurity Committee (JCC) member institution to dedicate the month for internal cybersecurity awareness sessions. He used the opportunity to encourage all other JCC member institutions to adopt such practices to aid in their internal cybersecurity readiness. Dr. Antwi-Boasiako recognised the contribution of the Ghana Armed Forces to Ghana's cybersecurity development, acknowledging three Senior Officers – Brig. Gen. A. Y. Nsiah, representing the Defence Intelligence, Col. A. K. Oduah, representing the Ghana Armed Forces Department of Defence Communication and Information Systems and Col. (Dr.) Tim Bataa-Banah representing the National Security Council Secretariat for their commitment to the Joint Cybersecurity Committee. He expressed the commitment of the CSA to work with the representatives towards achieving the mandate of the Ghana Armed Forces, "by ensuring your internal systems and network security and your national mandate to defend the territorial integrity of the Republic" He added that the theme of NCSAM



2022 was adopted to reflect the increasing need for cooperation among stakeholders to implement various provisions of the cybersecurity Act 2020 (Act 1038) to improve cybersecurity resilience in the country.

The Ag. Director-General re-iterated the five main strategic imperatives of the National Cybersecurity Policy and Strategy which focus on Building a Resilient Digital Ecosystem, Securing Digital Infrastructure, Developing National Capacity, Deterring Cybercrime and Strengthening Cooperation and with respect to the development of national capacity, he indicated that the strategy makes reference to the Development of Cyber Defensive Capabilities towards self-reliance. He further indicated that the Authority is committed to working with the Ghana Armed Forces and other members of the Joint Cybersecurity Committee to develop National Cyber Defence Programmes to serve as a blueprint for the development of national cyber capabilities to protect and defend Ghana's interest in cyberspace, to achieve a Secure and Resilient Digital Ghana.

He also assured GAF of continuous commitment to implement various applicable sections of the Cybersecurity Act, 2020 (Act 1038).

Remarks

Vice Admiral Seth Amoama
Chief of Defence Staff

Vice Admiral Seth Amoama stated that in recent times, cybersecurity issues had taken centre stage in global discourse because of its influence on transnational, regional and international security. He mentioned that modern trends in technology were incessantly evolving along with its accompanying opportunities and threats, and the Ghana Armed Forces was no exception.



Vice Admiral Seth Amoama
Chief of Defence Staff

He further indicated that in the military, cyberspace has emerged as the fifth domain of warfare alongside the traditional domains of land, sea, air and space. It is therefore not surprising that terrorists and violent extremists groups are using the internet as platforms to support their activities. Cybersecurity has therefore become a vital part of the operational effectiveness of militaries in the world, therefore "we acknowledge that cybersecurity is ingrained in the DNA of every armed force of today".

According to the Vice Marshal, the Ghana Armed Forces is taking steps to protect its Critical Information Infrastructure (CII) and assured the public that efforts are being made for every member of the GAF to understand the cyber threats, vulnerabilities and their impact on mission readiness.

Conclusion

The GAF Cyber Security Awareness Month was declared opened to give room for the commencement of the scheduled workshops, lectures, demonstrations and training sessions on essentials of cybersecurity and the implications of the use of social media by all ranks.

Official Launch of NCSAM 2022
Regulating Cybersecurity:
A Public-Private Sector Collaborative Approach



NATIONAL
CYBER SECURITY
AWARENESS MONTH

OFFICIAL LAUNCH OF NCSAM 2022- REGULATING CYBERSECURITY: A PUBLIC-PRIVATE SECTOR COLLABORATIVE APPROACH



Background

The Cyber Security Authority (CSA) on Monday October 3, 2022, launched its 2022 edition of the National Cyber Security Awareness Month (NCSAM) at the Cedi Conference Centre, University of Ghana, Legon. The Vice President of the Republic of Ghana, represented by Hon. Joseph Cudjoe, launched the event. The programme was attended by about 500 participants from the Government Sector, Industry, Civil Society Organisations, the Diplomatic Corps, the Media, among others.

Welcome Remarks

Dr. Albert Antwi-Boasiako
Ag. Director General, CSA

The Ag. Director-General for the Cyber Security Authority pressed on the need for local and international collaborations in tackling the borderless matters of cybercrimes and cybersecurity. He also noted that this was included in the Authority's mandate pursuant to Sections 13 and 14 of Act 1038, which authorises



Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

the establishment of a Joint Cybersecurity Committee (JCC); and Sections 81 of Act 1038 which establishes the Industry Forum. He further stated the importance of international cooperation in cybersecurity development as it has helped Ghana in reaching her cyber-related goals through joint exercises, intelligence sharing, and capacity-building programmes.

Dr. Antwi-Boasiako advised various stakeholders especially businesses, to invest about 15% to 20% of their ICT budget to implement effective cybersecurity measures for meaningful and sustainable progress in addressing cyber-related matters.

Remarks

Hon. Kojo Oppong Nkrumah
Minister for Information



Hon. Kojo Oppong's remarks called for the need to take advantage of the ongoing NCSAM 2022 activities. He stated that the Ministry of Information is looking forward to working with the Cyber Security Authority during the NCSAM celebrations and beyond to help raise awareness on the importance of effective cyber security measures.

Remarks

Hon. Albert Kan Dapaah
Minister for National Security



Hon. Albert Kan Dapaah stated that the theme for this year's NCSAM celebration gives Ghanaians a chance to reflect on the need for collaboration to ensure a safe nation. He highlighted on the need for private sector collaboration as they also play an essential role

in securing the country's cyberspace. He also pinpointed that the implementation of effective cybersecurity measures goes hand-in-hand with ensuring the nation's security, illustrating this through the fact that cybersecurity was part of the list of major security challenges in Ghana. He therefore urged the key players in Ghana's cybersecurity development to work together to develop systems that can address cybersecurity issues and protect the country as a whole.

Remarks

Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation



Hon. Ama Pomaa Boateng, Deputy Minister for Communications and Digitalisation, gave the remarks on behalf of the Minister for Communications and Digitalisation, Hon. Ursula Owusu-Ekuful. She acknowledged the importance of the theme of this year's edition of NCSAM, "***Regulating Cybersecurity: A Public-Private Sector Approach,***" as it accurately reflects the need for cooperation between the private sector and state actors, domestically and internationally, in cybersecurity. She also touched on the developments the Ministry is making to protect all stakeholders in cyberspace.

According to the Deputy Minister, Ghana's National Cybersecurity Policy and Strategy (NCPS) and the National Child Online Protection (COP) Framework are currently being revised with the goal of being implemented in 2023. She explained that the framework would provide a healthy digital environment for children, promoting the safe use of digital technologies. She also noted that cooperation is key to secure



Ghana's digital economy, noting the establishment of the Joint Cybersecurity Committee (JCC), pursuant to Section 13 of the Cybersecurity Act, 2020 (Act 1038) and its mandate to implement cybersecurity measures and promote a secure and resilient ecosystem. Additionally, she made note of the importance of the Memoranda of Understanding to be signed with the representatives from Rwanda and Mozambique, stating that this should encourage similar engagements with other sister African nations.



Keynote Address

H. E. Alhaji Dr. Mahamudu Bawumia
Vice President, Republic of Ghana

Hon. Joseph Cudjoe, Minister for Public Enterprises, representing His Excellency, the Vice President, Alhaji Dr. Mahamudu Bawumia, gave the keynote address to officially open the



2022 edition of NCSAM. In his address, Hon. Cudjoe noted that the need to build a resilient digital ecosystem is imperative for national development and even more so in the era of the 4th Industrial Revolution where new and emerging technologies and trends are "rapidly changing our daily lives". He further explained that these changes, although advantageous, have "exposed us to various threats". It was on this note that he urged Ghanaians, both businesses and individuals, to "develop the needed cybersecurity consciousness to help mitigate cybercrimes, which according to statistics are caused by human actions in about 90% of the cases."

He emphasised the need to implement the provisions of the Directive for the Protection of Critical Information Infrastructure and added that effective January 2023, all Critical Information Infrastructure Owners, whether public institutions or private sector, would be required to undergo mandatory compliance checks and audits to ensure the protection of Ghana's critical systems.

He acknowledged the role of international cooperation in the development of cybersecurity and indicated "as cyberspace is borderless and its interdependencies keep widening, Ghana is committed to improving collaboration not only at the domestic level but internationally in the fight against cybercrimes. I commend all international and local partners who have been instrumental in Ghana's cybersecurity development so far."

In conclusion, Hon. Joseph Cudjoe acknowledged the presence of the delegation from the National Cyber Security Authority of Rwanda led by Colonel David Kanamugire and the National Information Communication Technology Institute of Mozambique led by Professor Lourino Alberto Chemane who joined Ghana for the launch of NCSAM 2022 and for the signing of a Memorandum of Understanding for cooperation with Ghana on cybersecurity. issues.

SIGNING OF MEMORANDA OF UNDERSTANDING (MOUs) WITH MOZAMBIQUE AND RWANDA





Memoranda of Understanding (MoUs) were signed between Ghana (represented by the Ag. Director-General of the Cyber Security Authority) and Rwanda (represented by Colonel David Kanamugire, CEO of the Rwandan National Cyber Security Authority), and between Ghana and Mozambique (represented by Professor Lourino Alberto Chemane, Board Chairman of the National Information and Communications Technology Institute of Mozambique). These MoUs are a show of commitment between the countries and their dedication to work together to raise the cybersecurity profile in their respective countries and the continent as a whole. The signing was witnessed by the Minister for Public Enterprise, Minister for Information and the Deputy Minister for Communications and Digitalisation.

High-Level Panel Discussion

There was also a high-level Panel Discussion on Cybersecurity Cooperation. The Panel comprised Dr. Albert Antwi-Boasiako, Prof. Lourino Alberto-Chemane, Colonel David Kanamugire, and the Ambassador of the State of Israel to Ghana, H.E. Shlomit Sufa. The discussions were moderated by Mr. John Awuah, CEO of the Ghana Association of Banks.

The Panelists shared their views and experiences on cybersecurity developments in their respective countries and the importance of domestic and international cooperation in these efforts.



Conclusion

The event came to an end with closing remarks by Madam Patricia Adusei-Poku, Executive Director of the Data Protection Commission and the vote of thanks was delivered by Justice Afia Serwah Asare-Botwe, a member of the Joint Cybersecurity Committee.

Public Consultation on Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals

NATIONAL
CYBER SECURITY
AWARENESS MONTH

PUBLIC CONSULTATION ON FRAMEWORK FOR THE LICENSING OF CYBERSECURITY SERVICE PROVIDERS, ACCREDITATION OF CYBERSECURITY ESTABLISHMENTS AND ACCREDITATION OF CYBERSECURITY PROFESSIONALS



Background

The Public Consultation on the Framework for the licensing of Cybersecurity Service Providers (CSPs), the accreditation of Cybersecurity Establishments (CEs) and the accreditation of Cybersecurity Professionals (CPs) was organised to receive inputs for the Framework that will serve as guidance and direction to CSPs, CEs and CPs. The framework is necessary to provide a streamlined mechanism for ensuring that cybersecurity service providers offer services in accordance with approved standards and procedures in line with the Cybersecurity Act, 2020 (Act 1038) and international best practice and it is also expected to raise the quality of cybersecurity service providers, to improve and maintain standards that offer baseline protection to the systems within Ghana's digital ecosystem.

Opening Remarks

Mr. Alexander Oppong
Lead, Capacity Building and Awareness Creation (CBAC),
Cyber Security Authority (CSA)

Mr. Alexander Oppong welcomed participants who came from various institutions including academia, industry, and Government. He thanked them for taking time off their busy schedules to participate in the public consultation. He added that the public consultation on the Framework was part of efforts to improve understanding and



Mr. Alexander Oppong
Lead, Capacity Building and Awareness Creation (CBAC),
Cyber Security Authority (CSA)

collaboration towards the effective implementation of relevant provisions in the Cybersecurity Act, 2020 (Act 1038).

Mr. Oppong affirmed that it is the responsibility of cybersecurity professionals, cybersecurity service providers and cybersecurity establishments to protect the IT infrastructure, networks, systems, and data of clients from attacks and breaches. He further indicated that, the Cybersecurity Act,2022 provides for the regulation of the industry to ensure accountability and standardisation. He therefore called on all participants to contribute towards the Framework.

Remarks

Dr. Albert Antwi-Boasiako
Ag. Director General, CSA



The Acting Director-General of the Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako began his address by making special mention of some Board Members of the Authority, Mr. Carl Sackey, Mrs. Adelaide Benneh-Prempeh, and Mrs. Mavis Vijaya Afakor Amoa for their extraordinary commitment in participating in the public consultation. He also thanked the staff of the CSA, the Committee established for the development of the framework, and other key stakeholders who worked tirelessly to contribute to the drafting of the Framework for the Licensing of CSPs,

accreditation of CEs and accreditation of CPs. Dr. Antwi-Boasiako mentioned that the Cyber Security Authority is responsible for working with industry players to ensure the effective implementation of Act 1038, by setting standards and guidelines for the industry players. He opined that the process of regulating sector is important as it set to provide sanity and orderliness just like other professions. He added that the services provided by cybersecurity professionals are intrusive in nature and it was therefore important to assess the credibility of persons offering these services.

Presentation

Madam Jenifer Mensah
Lead, Legal and Compliance, CSA

Madam Jenifer Mensah gave a presentation on the draft Framework, explaining into detail the key elements of the framework and how it was expected to bring sanity into industry.

In her presentation, she explained that prior to the promulgation of Act 1038, no government institution had the mandate to regulate CSPs, CEs and CPs in the country. She added that the CSA pursuant to Sections 49, 50,51,57 & 59 of Act 1038, is in the process of developing a framework for licensing CSPs, accreditation of CEs and the accreditation of CPs hence the public consultation to seek the inputs and contributions of industry on the framework.



She added that it is important to regulate CSPs, CEs and CPs to prevent the abuse or exploitation by less credible CSPs, CEs and CPs who may gain knowledge of existing vulnerabilities and sensitive information of clients. She indicated that the process was also important to prevent substandard processes from being used by CSPs, CEs and CPs to the detriment of Ghana's Digital Ecosystem and it will prohibit incompetent CSPs and CPs from managing critical information assets of clients. She was further confident that the regulatory process will support businesses and Government agencies to identify credible CSPs, CEs and CPs and ensure those who undertake critical services are in good standing in accordance with cybersecurity regulations.

Submissions by Participants

Mr. Carl Sackey, a Member of CSA's Governing Board, representing the Industry Forum, noted that the licensing and accreditation of cybersecurity service providers, establishments and professionals was necessary to manage risks and to ensure professionalism in the cybersecurity ecosystem.

Mrs. Mavis Vijaya Afakor Amoa, the Director of the Legislative Drafting Division at the Office of Attorney-General and Ministry of Justice and





also a member of the CSA Governing Board, shared some insights on the importance of the exercise and called on participants to contribute objectively to the development of the framework. She further assured the public that the framework will ensure fairness to all applicants and provide mechanisms to address grievances that may arise.



Madam Adelaide Benneh-Prempeh, another member of the CSA Governing Board, encouraged industry players to focus on the brighter side of the framework and look forward to the development of the cybersecurity profession to its full potential.

Questions & Answers

During the questions and answers session moderated by Dr. Albert-Antwi Boasiako, Mr. Eliasu of Republic Bank, Ghana enquired whether there would be an exam before the accreditation of professionals. Mr. Edem Glymin of Global Secure Solutions also enquired of the proposed fees to be charged while Mr. Abubakar Issaka of Cyberwatch and Data Protection Ghana, sought to know the timelines concerning the process of acquiring a licence. He further enquired on how licensed service providers and cybersecurity professionals could leverage on the Africa Continental Free Trade Area (AfCFTA) project.



Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Dr. Antwi-Boasiako, in his response to the questions raised, mentioned that for the start, technical competencies, certifications, years of experience and due diligence will be the metrics to be used in assessing and granting an accreditation instead of an examination. He was quick to add that participants needed to look at the licencing in a progressive manner, starting with the securing and protection of Critical Information Infrastructure (CII) and government institutions. On the issue of proposed fees, he stated that it was still under consideration. Regarding leveraging on the African Continental Free Trade Area (AfCFTA), Dr. Antwi-Boasiako posited that, there were already engagements with other countries in Africa on cybersecurity related matters. He cited the signing of the Memoranda of Understanding (MoU) with Mozambique and Rwanda.

Continuing with the discussions, Mr. C.K. Bruce of Innovare expressed the concern that the global shortage of cybersecurity skillset affects Ghana, hence focus should be on protecting and developing the cyber industry. Mr. Daniel Gyampo, President of ISACA Ghana advocated that the CSA should have a database of cybersecurity professionals on its website.

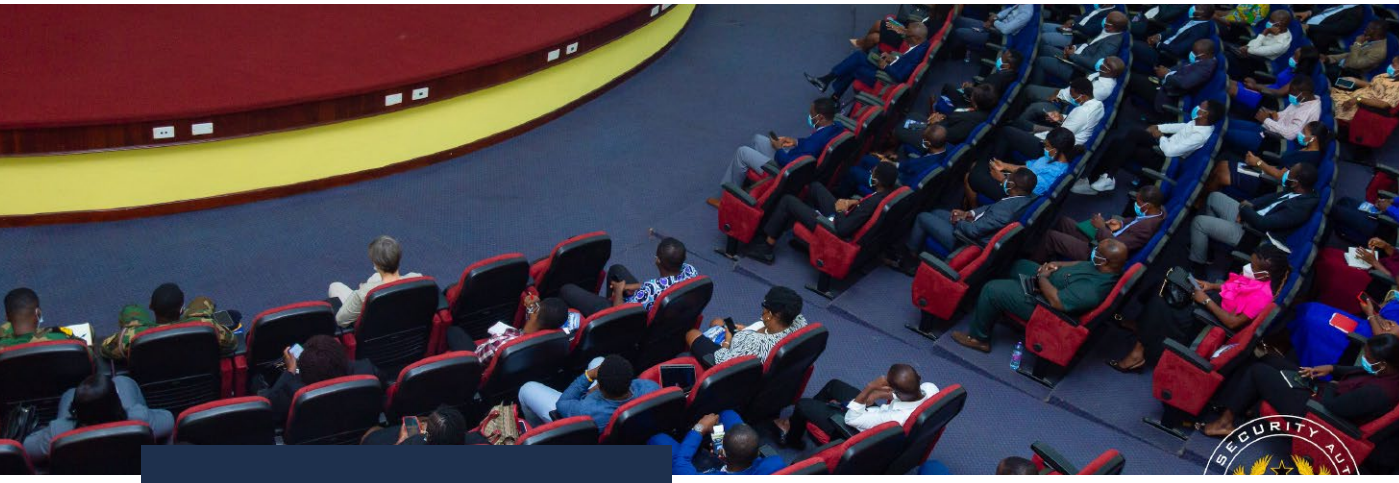
Dr. Antwi-Boasiako shared the concept of the tier system with participants. He explained that the tier system is a ranking system and mechanism to categorise CSPs, CPs, and CEs based on competency levels among other factors. It was largely agreed that the tier system should be applied to CSPs and CEs but not for CPs as it was too complex for a start. Majority of the participants also consented to tier 1 being the highest level and tier 3 being the lowest level. There was also a consensus that a cybersecurity professional who operated within the territory of Ghana, needed to be licensed.

It was explained that existing cybersecurity service providers and cybersecurity establishments would be given a grace period of three months to comply with the Framework which would be effective from January 2023. The Public Consultation ended with a vote of thanks by Madam Ingrid Serwah Asare of the Legal and Compliance Unit of the CSA.

Forum on Ghana's Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals

NATIONAL
CYBER SECURITY
AWARENESS MONTH

FORUM ON GHANA'S CYBERSECURITY REGULATIONS AND OPPORTUNITIES FOR CYBERSECURITY INDUSTRY PLAYERS AND PROFESSIONALS



Background

Sections 49-56, 57-59, and 82 of the Cybersecurity Act, 2020 (Act 1038) directly impacts the work of cybersecurity service providers and professionals who play a crucial role in Ghana's cybersecurity development. To effectively implement the above-mentioned provisions of the Act, the Cyber Security Authority (CSA) in collaboration with the Institute of ICT Professionals GH organised a Forum on Ghana's Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals to engage stakeholders in the cybersecurity ecosystem to explore opportunities in cybersecurity regulations.

Opening Remarks

Mr. Carl Sackey
Member, CSA Governing Board

Mr. Carl Sackey welcomed everyone to the event and reiterated the purpose of the Forum and its importance to industry players. He further spoke about the essence of regulations in cyberspace and the need to protect the interest of citizens and the country at large. He encouraged the industry players to take advantage of the cybersecurity regulatory regime as it will ensure a level playing field that fosters hard work and gives assurance to all.





Presentation

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Dr. Albert Antwi-Boasiako, acting Director-General of the CSA, extended a warm welcome to everyone and acknowledged the industry's contribution to cybersecurity development over the years.

In his presentation, he indicated that the private sector had taken the lead in terms of awareness creation and building standards to secure the digital ecosystem before the Authority came into existence and that their efforts contributed to Ghana's rating of 86.69% by the 2020 ITU Global Cybersecurity Index (GCI).

He briefed the participants on the Framework for the licensing of Cybersecurity Service Providers (CSPs), the accreditation of Cybersecurity Establishments and the accreditation of Cybersecurity Professionals (CPs) which has undergone various consultation stages and on the fact that, the regulatory regimes will present various opportunities for personnel in the field of cybersecurity. He encouraged young people to take advantage of these opportunities to develop careers in cybersecurity. Among the benefits to be derived, he noted employment opportunities, the provision of a streamlined mechanism for cybersecurity practitioners to meet both legal and national security requirements while addressing cybercrime and cybersecurity issues and the creation of businesses for cybersecurity service providers and cybersecurity professionals.

According to Dr. Antwi-Boasiako, it is important to balance the needs of National Security and those of citizens and businesses. He therefore urged the professionals to collaborate with the CSA for the effective implementation of the relevant provisions of the Cybersecurity Act, 2020 (Act 1038) which includes regulations on the licensing of Cybersecurity Service Providers (CSPs), the accreditation of Cybersecurity Establishments (CEs), the accreditation of Cybersecurity Professionals(CPs), the accreditation of sectoral Computer Emergency Response Teams(CERTs), and regulations on the industry forum and the operationalisation of the Cybersecurity Fund.

Questions and answers

- A participant asked if Ghana has an incidence response level 3 to undertake investigations and forensics to identify kinds of attacks or incidents.
- Dr. Albert Antwi-Boasiako responded by saying that, cybersecurity is multisectoral and hence the establishment of the Joint Cybersecurity Committee. He encouraged participants to read Section 13 of the Cybersecurity Act, 2020 (Act 1038). He added that, the question lies in the mandate of the National Security and that every government agency has its given mandate within which it operates.
- A participant commended the Cyber Security Authority and asked about the plans of the Authority to assist academia in the setting up departments to train experts in cybersecurity and if these academic institutions offering courses in cybersecurity would be regulated.
- Mr. Carl Sackey stated in response that it is a work in progress and that it is part of what the Industry Forum seeks to achieve, adding that there is already a representative from academia on the CSA Governing Board to help facilitate discussions on the issue for implementation.
- A participant asked if there would be opportunities for cybersecurity enthusiasts who have no information technology background to have careers in cybersecurity.
- Mr. Carl Sackey responded that everyone regardless of their professional background can take a course in cybersecurity provided that adherence to the regulations of the profession is ensured.
- A participant asked whether in the process of licensing of Service Providers the professionals that work with these service providers could be licensed alongside their institutions. He also sought to find out if provisional licenses would be issued during the period of acquiring the licence.













- Madam Adelaide Benneh Prempeh responded by indicating that Act 1038 specifies a period under the transitional provisions for those who are practicing as Cybersecurity Professionals to obtain licenses. She added that the requirements and processes to apply for a license will come with reasonable time frames which will not necessarily go against applicant. With respect to the issue of provisional licences, she indicated that there would be a problem if a provisional license is granted to someone who does not qualify to be licensed. She was optimistic that licences would be given to all those who qualify when the process commences.



Conclusion

The participants expressed appreciation for the presentations and the insights given on the Cybersecurity Act, 2020 (Act 1038) and how they would be affected by the respective regulations.

They were encouraged to set-up the Industry Forum with guidance from the CSA to help improve information sharing and to help improve collaboration between the Authority and industry players especially those in the private sector.

Public Consultation for the Development of an Accreditation Framework to Accredit Sectoral Computer Emergency Response Teams (CERTs)



NATIONAL
CYBER SECURITY
AWARENESS MONTH

PUBLIC CONSULTATION FOR THE DEVELOPMENT OF AN ACCREDITATION FRAMEWORK TO ACCREDIT SECTORAL COMPUTER EMERGENCY RESPONSE TEAMS (CERTS)



Background

As part of measures to achieve effective cybersecurity incident response and coordination, the Cyber Security Authority (CSA) is mandated to establish Sectoral Computer Emergency Response Teams (CERTs) to collect, collate and coordinate responses to cybersecurity incidents within sectors pursuant to Section 44(1) of the Cybersecurity Act, 2020 (Act 1038). Pursuant to Sections 44(4) and 59 of Act 1038, the CSA is mandated to accredit and oversee the operations of Sectoral CERTs.

To implement this provision, the CSA aims to develop an accreditation framework to accredit Sectoral CERTs to effectively streamline operations of the Sectoral CERTs given their criticality and developments with respect to cybersecurity in the country.

A Public Consultation was thus organised to convene industry players, stakeholders, academia, Government, private sector and civil society organisations to collectively make inputs for the development of the Accreditation Framework.

Opening Remarks

Mr. Benjamin Ofori
Lead, Critical Information Infrastructure Protection, CSA

Mr. Benjamin Ofori, the Lead for the Critical Information Infrastructure Protection Unit of the CSA welcomed participants and highlighted the



Mr. Benjamin Ofori
Lead, Critical Information Infrastructure Protection, CSA

importance of the session. He mentioned that the event was expected to be an interactive one, where participants would make the needed inputs towards developing and shaping the Framework for the Accreditation of Sectoral CERTs. He described the CERT as the heartbeat or nerve centre of cybersecurity meaning a CERT is the converging point for the people, processes, and technology principles of cybersecurity which must be given the needed attention.



Remarks

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Dr. Albert Antwi-Boasiako, the Acting Director-General of the CSA, in his remarks thanked all participants for joining the session and specially thanked the committee and the CSA team that worked on drafting the Sectoral CERTs Accreditation Framework.

Dr. Albert Antwi-Boasiako further indicated that, the CSA's approach to work with stakeholders in the industry for cybersecurity development in the country, which started about six (6) years ago, has since made very remarkable strides. He added that Ghana is adopting a decentralised incident response mechanism which has proven to be more effective than the centralised system. The decentralised system for incident response best fit the Ghanaian ecosystem as there were already many vibrant regulators in the system and hence, it was reasonable to leverage on the existing regulatory bodies for collaboration and to reduce bureaucracies.

Speaking on the legal framework for the Sectoral CERTs, he indicated that an accredited Sectoral CERT would give the Sector CERT the legal powers to have oversight on its constituents. He explained that measures will be put in place to second members of one CERT to another CERT to help in the capacity building of officers.

Dr. Antwi-Boasiako mentioned that the CSA looks forward to a more collaborative approach with respect to regulatory compliance rather than an imposition. He went on to emphasise Ghana's commitment to having one of the most efficient incident response systems in place and called for serious commitment at the domestic level. He encouraged stakeholders to seek the creation of an industry that is appealing to current and future generations.

Submissions by Participants

Professor Yeboah Boateng of the National Communications Authority (NCA) stated that the cybersecurity framework was very essential, and



the timing was right. He called for an agile cybersecurity regulation, the need to be up to date with cybersecurity needs and development and finally, the framework ought to be human centred and future looking.



Madam Adelaide Benneh-Prempeh, a legal practitioner and member of the CSA Governing Board, in her remarks stated that the CSA is a forward-looking institution and asked participants to open up and contribute to developing the framework as it would go a long way towards achieving a safer digital space.

Presentation

ACCREDITATION FRAMEWORK FOR SECTORAL CERTS
Madam Jenifer Mensah
Lead, Legal and Compliance, CSA



She outlined the importance and objectives as well as critical areas of the draft framework. She stated emphatically that the framework was necessary because it sought to regularly assess



and monitor the technical competencies, reliability, and integrity of Sectoral CERTs; effectively ensure compliance of regulatory directives; effectively streamline operations of Sectoral CERTs; and, to ensure strong trusted working relationships between the Sectoral CERTs and the National CERT.

Questions and Answers

Professor Yeboah Boateng of the National Communications Authority suggested that the duration of the licence should be made 5years instead of 2years as that will help the Sectoral CERTs commit to it financially. In response, Madam Adelaide Benneh-Prempeh, a member of the CSA Governing Board, said that the duration of two years was binding by the Cybersecurity Act, 2020 (Act 1038) and so if there was going to be a change it would have to go through the Parliament of Ghana. She further indicated that though it would not be new for an Act to be amended within its early stages of implementation, the current provisions were however good to begin with.



Mr. Charles Osei Bonsu of the Bank of Ghana (BoG) was interested in knowing how the personnel were going to be assessed. In response, Dr. Albert Antwi-Boasiako mentioned that the guidelines for assessing personnel was outlined in the framework and added that aside background checks, the personnel who would be working in the CERTs must have a good mindset for the cybersecurity environment.



Mr. Ernest Boateng of the Financial Intelligence Centre (FIC) sought clarification on which Sectoral CERT the FIC would be reporting their incidents to. Dr. Antwi-Boasiako answered by saying that, the FIC should be reporting to the National Security Sectoral CERT.

Conclusion

It was concluded at the event that by January 2023, the framework for accreditation of Sectoral CERTs will be implemented.

Compliance Workshop on the Directive for the Protection of Critical Information Infrastructure (CII) for CII Owners

NATIONAL
CYBER SECURITY
AWARENESS MONTH

COMPLIANCE WORKSHOP ON THE DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII) FOR CII OWNERS



Background

The purpose of the workshop was to establish the compliance obligations of Critical Information Infrastructure (CII) Owners with the Directive for the Protection of CII whilst fostering collaboration and partnership efforts with the Owners for the effective implementation of CII directives and initiatives.


Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Remarks

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Dr. Albert Antwi-Boasiako mentioned that the CSA has been designated as a security sector agency and thus a part of the national security architecture. He further stated that cybersecurity threats have become central amongst many other security threats in the country. In that regard, the CSA has to collaborate with other institutions to control cybersecurity threats. He defined regulation with regards to the CSA's mandate as setting standards, complying to certain disciplines, obtaining best practices, and customising them to fit the solution of respective cybersecurity issues. He added that as the regulator of cybersecurity in Ghana, the CSA will be working with other sectoral regulatory bodies and industry players to comprehend best practices in combatting cybersecurity issues.

The Ag. Director-General explained that the common goal for all participants present

whether they belong to the private sector or public sector was to contribute to protecting critical systems by deterring cybercrime, securing digital networks, ensuring business continuity and boosting confidentiality, integrity, and availability of information systems or assets.

He added that the government is responsible for putting in enabling interventions and to demonstrate leadership through the CSA. He further indicated that the enabling interventions are the Cybersecurity Act, 2020 (Act 1038) and the Directive for the Protection of Critical Information Infrastructure (CII).

Dr. Antwi-Boasiako thus encouraged all CII Owners to work collectively, as an attack on a CII institution may likely have a devastating impact on the socio-economic well-being of citizens and national security. He elaborated on the necessity of the CII registration process encouraging all CII owners to comply.



Remarks

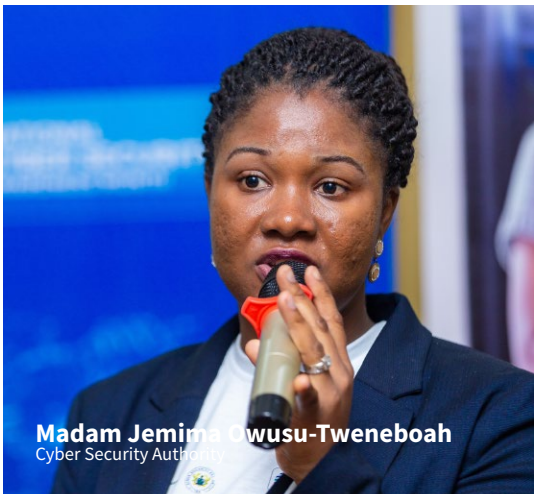
Mr. Benjamin Ofori
Lead, Critical Information Infrastructure Protection, CSA

Mr. Ofori welcomed all participants and expressed his gratitude for their presence at the workshop. Mr. Ofori elaborated that the Act provides the basis for multistakeholder engagements for effective collaborations and partnerships for the country's cybersecurity development. He added that the objective of the Directive is to operationalise the provisions of Sections 35 to 40 and Section 92 of the Cybersecurity Act, 2020 (Act 1038). He encouraged CII owners to comply with the Directive for the Protection of CII and the Cybersecurity Act, 2020.

Presentation

DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE
Mad. Jemima Owusu-Tweneboah,
Mr. Eugene Sackey
Cyber Security Authority (CSA)

Madam Jemima Owusu-Tweneboah and Mr. Eugene Sackey presented on the Directive for





the Protection of Critical Information Infrastructure. The presentation elaborated on policies, baseline cybersecurity requirements, technical and organisational measures, incident reporting procedures necessary for managing cybersecurity issues.

They also stated that a designated CII owner must conduct an internal audit to ensure compliance with the Directive and submit copies of audit reports to the CSA. Participants were informed that failure to comply with the Directive will attract applicable criminal and administrative sanctions as provided in the Cybersecurity Act, 2020 (Act 1038) and other relevant enactments.

Questions and Answers

Mr. Francis Donkor of the Ghana Ports and Harbours Authority (GPHA) asked if the CSA is going to depend on existing auditing reports of a respective institution registered with International Standards Organization (ISO) 27001 during the CSA's auditing and compliance process. Dr. Antwi-Boasiako responded that the CSA will leverage on existing best practices by which ISO 27001 is a part of. He added that cybersecurity professionals in various institutions will be vetted and accredited, while cybersecurity service providers will be licensed by the Authority. He admonished institutions to give the CSA visibility on business operations.

A representative from the University of Professional Studies, Accra (UPSA) asked how the CSA was going to regulate private cybersecurity professionals in the country. Again, Dr. Antwi-Boasiako responded that the CSA is working with all 13 designated sectors and explained that private sector institutions and institutions abroad that provide cybersecurity services within the country will have to register with the CSA and comply with the regulatory requirements.







Mr. Reuben Tetteh from National Identification Authority (NIA) asked if the CSA has a specific format for incident reporting for CII owners. Madam Jemima Owusu-Tweneboah retorted that CSA will provide a template form online for incident reporting. However, reporting through other media such as email, WhatsApp will be dutifully attended to.

A representative from the Consolidated Bank, Ghana (CBG), asked how responsible disclosures are handled by the CII Directive on incident response situations. Mr. Gerald Awadzi in answering referred to section 5.3b of the CII Directive which provides the baseline requirement for incident reporting. He reiterated that incidents from CII owners must be reported to their Sectoral CERT for onward submission to the National CERT.

Mr. Bright Ohene stated that the CII Directive does not have timelines for implementation making reference to Bank of Ghana's Cyber and Information Security Directive which included timelines for implementation of the Directive. Mr. Benjamin Ofori in response stated that the compliance of the Directive, was initially slated for on October 1, 2022, would take effect fully from January 1, 2023, on the request of the CII Unit of the CSA.

Mr. Kwame Sam Biney from Anglogold Ashanti asked if reporting of incidents to Sectoral CERTs is for information purposes only or for support and response. Madam Owusu-Tweneboah responded by stating that the mandate of the CSA includes provision of support and guidance to CII owners pursuant to the implementation of the CII Directive and the Cybersecurity Act, 2020.

Mr. Godwin Kofi Cudjoe from Huawei S.A. Technologies (Ghana) Limited asked if they can be designated as a CII owner and refuse to register their infrastructure since their infrastructure is operated in silos. In answering, Mr. Gerald explained that Huawei S.A. Technologies (Ghana) Limited and other institutions with similar situations will be engaged by the CSA to deliberate further on their circumstances.

Mr. Kwesi Bamfo from Bui Power Authority asked how the CSA plans to assist CII institutions such that cybersecurity can be regarded as a priority at the governance level for decision making instead of it being the burden of IT Departments. Mr. Awadzi responded that Section 5.1c of the CII Directive empowers accredited cybersecurity professionals to discuss with the Board and Management of their respective organisations on matters of cybersecurity. He added that the CSA does not specify best practices for respective CII Owners. CII Owners may use best practices suggested by regulators and any other international best practices necessary for cybersecurity.


Madam Adelaide Benneh-Prempeh
Member, CSA Governing Board

Recommendations

Mrs. Adelaide Benneh Prempeh, recommended that CII owners should work together to gain trust to contribute towards building the national cybersecurity posture.

Dr. Albert Antwi-Boasiako recommended that internal cybersecurity exercises and assessment be performed by CII owners to aid in contributing to the effective management of cybersecurity issues.

The Maiden Edition of The National Cybersecurity Challenge (NCC) for Senior High Schools

NATIONAL
CYBER SECURITY
AWARENESS MONTH

THE MAIDEN EDITION OF THE NATIONAL CYBERSECURITY CHALLENGE (NCC) FOR SENIOR HIGH SCHOOLS



Background

Ensuring online safety for children and young people has gained national prominence, triggering stakeholder consultations and the promulgation of Child Online Protection (COP) provisions in the Cybersecurity Act, 2020 (Act 1038). As part of efforts to sustain awareness creation and promote cybersecurity among children, the Cyber Security Authority organised the maiden National Cybersecurity Challenge (NCC) as part of the 2022 National Cyber Security Awareness Month.

The event brought together students from selected Senior High Schools to compete in cybersecurity quizzes and problem-solving exercises, and to demonstrate practical knowledge on online safety topics on the theme; 'Cyber Safety and Protection - Our Collective Responsibility.'

The participating schools were: Adisadel College, Mfantsiman Girls' Senior High School, Northern School of Business, Oda Senior High School, Presbyterian Boys Senior High School, and St. Monica's Girls Senior High School. Other schools were in attendance to support and cheer the participants and they included, Kinbu Secondary Technical High School, Accra Girls Senior High School, Wesley Girls Senior High School, Accra High School, and Odorgonno Senior High School.

Welcome Address

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Delivering the welcome address on behalf of the Ag. Director-General of the Cyber Security Authority, Madam Afua Brown-Eyeson welcomed the participants, supporters, and educators to the maiden edition of the National Cybersecurity Challenge.

She particularly thanked the students and teachers from the participating Senior High schools for accepting the invitation to be part of the pilot event; adding that, “these schools have been selected for this maiden challenge



because they have committed themselves to set up Cybersecurity Clubs and used the opportunity to encourage other schools to engage with the CSA for similar projects. From next year, there will be regional cybersecurity challenges.”

According to Ms. Brown-Eyeson the objective of the National Cybersecurity Challenge is to “create awareness on cybersecurity best practices for students, encourage them to stay safe online, sensitise them on career opportunities in cybersecurity and ultimately, develop a cybersecurity culture among young children”.

She indicated that access to the internet offers children and young people unprecedented opportunities to communicate, connect, learn, and access information from different parts of the world, but these opportunities come with new security challenges.

According to Madam Brown-Eyeson, a survey conducted by the CSA in February 2022 in selected Senior High Schools within the Greater Accra region showed that out of 3,622 students, 2,331 had encountered sexual content; 2,025 have met online strangers physically; and 769 of these students had experienced cyberbullying.

She urged law enforcers, parents, guardians, and teachers to take proactive efforts to ensure children are safe online.

She further indicated that the Authority is developing a National Child Online Protection Framework aimed at tackling the incidents of Child Online Sexual Exploitation and Abuse, child sexual abuse materials, online harassment, and cyberbullying against children.



The Framework will be enforced in conjunction with the provisions of Sections 62-66 of the Cybersecurity Act, 2020 (Act 1038) and other international conventions, to provide guidelines on how children can stay safe online and punish all who abuse the rights of children online.

Remarks

Mr. Fianchra McAsey
Deputy Country Representative, UNICEF Ghana

Mr. Fianchra McAsey, in his remarks, congratulated Ghana, through the CSA, for the launch of the National Cybersecurity Challenge and for the determination to promote Child Online Protection. Mr. McAsey explained that as



children continue to gain access to the internet, they become susceptible to numerous risks and threats, adding that the event is appropriate and timely.

He stated that UNICEF-Ghana is proud to be associated with Ghana's Child Online Protection campaigns. He called on all stakeholders, including the private sector, to collaborate with the CSA in ensuring that every child enjoys a safe online experience.

Keynote address

Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation

Hon. Ama Pomaa Boateng in her keynote address, noted that "the internet has become a critical tool for communication and education in today's world. As internet usages advance however, there are several crimes being committed in that space and we all have individual and collective responsibilities to help address some of the challenges to promote a safe and positive use of digital technologies, especially among children and young people."



According to the Deputy Minister, children are among the vulnerable in society, making them susceptible to threats such as cyberbullying, cyberstalking, phishing attacks, and sextortion, amongst others. Such malicious activities undermine a child's freedom, which is why they are at the forefront of government's national cybersecurity efforts. She also pointed out that collaboration is essential in the development of cybersecurity in Ghana, especially among



children, citing Ghana's partnership with UNICEF-Ghana and the Internet Watch Foundation (IWF) as examples.

Hon. Pomaa Boateng highlighted the fact that children can only be made aware of the dangers the cyberspace brings through education. She was optimistic that the National Cybersecurity Challenge can help promote the needed education and awareness for the safe and positive use of digital technology by children and young people and inspire a national conversation about using technology responsibly.

She encouraged the young students to take advantage of the cybersecurity education they receive from their various Cyber Clubs and to consider taking on cyber-related careers in the near future.

The National Cybersecurity Challenge

The National Cybersecurity Challenge had six competing schools fighting for the trophy and bragging rights of being the Cyber Hero of the maiden edition of the event. Mr. Dan Afari Yeboah, of "What Do You Know?" fame was the Quizmaster of the Challenge.

The quiz was divided into three rounds. The first round was a speed round consisting of 30 multiple-choice questions, of which each school was required to answer a total of five questions. The second round was a "Question of the Day" problem, while the last round consisted of riddles the contestants needed to unravel. The quiz focused on various cybersecurity topics, such as social engineering, online safety, and the Cybersecurity Act, 2020 (Act 1038).

At the end of the contest, Presbyterian Boys Senior High School won the Challenge with 64 points, Mfantsiman Girls Senior High School came 2nd place with 59 points, Adisadel College was 3rd with 57.5 points, St. Monica's Girls Senior High School had 54 points, Oda Senior High School had 50 points and Northern School of Business had 42 points.

Closing Remarks

Madam Afua Brown-Eyeson
Lead, Child Online Protection, CSA

In bringing the event to a close, Ms. Afua Brown-Eyeson thanked participants for their enthusiasm and dedication to ensuring the success of the event. She also encouraged other schools to engage with the CSA to establish Cyber Clubs to ensure their participation in the Challenge next year. She thanked special guests for gracing the programme and sponsors for their impeccable support.

Civil Society Forum on Regulating Cybersecurity through Strategic Partnership



NATIONAL
CYBER SECURITY
AWARENESS MONTH

CIVIL SOCIETY FORUM ON REGULATING CYBERSECURITY THROUGH STRATEGIC PARTNERSHIP



Background

Cybersecurity risks in the operations of Civil Society Organisations (CSOs) in Ghana have not been explored and documented due to lack of capacity and expertise, although these organisations rely on a range of systems, networks, and applications for their work. According to the World Bank, 10.5 million records are lost or stolen every month; 438,000 every hour, and a single large-scale attack can trigger $53 billion in economic losses. Regarding developing countries, the African continent is among the fastest-growing regions in terms of cybercrime activities, with the World Economic Forum declaring cybercrime as one of the region's greatest threats. Additionally, in 2020, it was estimated that Africa has a shortage of 100,000 proficient cybersecurity personnel. In January 2022, Ghana was ranked 3rd globally regarding the use of social media usage, an indication of reliance on the internet for all sectors of life including education, lifestyle, businesses, and entertainment hence susceptibility to cybercrime.

In view of this, the Cyber Security Authority (CSA) in collaboration with GIZ Ghana organised a Forum on Strategic Partnerships with relevant Civil Society Organisations on cybersecurity awareness to provide practical and technical analysis to CSOs on the threats, risks and opportunities of emerging technology in building synergies among all stakeholders to ensure compliance of cybersecurity regulations.

Welcome Remarks

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Giving the welcome remarks on behalf of the Ag. Director-General of the CSA, Dr. Albert Antwi-Boasiako, Mr. Benjamin Ofori, welcomed all participants and noted that the Forum was important due to the increasing reliance on the internet by citizens for various activities including education, work, business, and entertainment.

Mr. Ofori revealed that, as the use of digital technologies increases, so does the prevalence of cybercrime. Cybercriminals take advantage of vulnerabilities to target individuals, companies, and organisations; thereby jeopardising confidentiality, integrity, and availability of systems and networks, including Critical Information Infrastructure. He added that numerous obligatory cybersecurity regulations have been established following the passage of the Cybersecurity Act, 2020 (Act 1038) as part of measures to ensure a secured and safe cyber ecosystem.



Mr. Ofori pointed to the fact that collaborative regulations hold the key to bringing both public and private sector stakeholders together towards achieving a secure and resilient digital Ghana. He urged Civil Society Organisations to share relevant information and serve as a mouthpiece to create the needed awareness on online safety and other related matters.



Remarks

Mr. Sampson Kwakwa
Technical Advisor, Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ)

Mr. Sampson Kwakwa, in his remarks, indicated that GIZ has actively supported Ghana in reducing Financial Crimes by collaborating with agencies such as the Economic and Organised Crime Office (EOCO) and the Ghana Police Service in prosecuting cybercrime cases.

He said the Forum would provide participants with knowledge on identifying threats, mitigating cybersecurity risks, and create an opportunity to have and build a healthy working partnership for the protection of the cyber ecosystem.



Remarks

Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation

Hon. Ama Pomaa Boateng expressed her appreciation to the CSA and GIZ for organising such an important Forum. The Deputy Minister explained that the Forum is an indication of Government's appreciation of the role of CSOs in the socio-economic development of the country and its commitment to collaborating with CSOs on cybersecurity development in Ghana.

She elaborated on the fact that digital technologies have increasingly become integral to the effective functioning of societies worldwide, noting that although Ghana has come a long way in its efforts to digitalise the economy in unison with the digital revolution, digitalisation efforts cannot be sustained without the development of cybersecurity.

According to Hon. Pomaa Boateng, as CSOs rely on digital technology and the internet for their operations and service delivery, they are increasingly faced with sophisticated attacks such as ransomware and phishing, and other financially motivated cyberattacks which were hitherto mainly targeted at public and private sector organisations. She thus urged the CSOs to work towards cyber resilience as a necessity in ensuring organisational resilience.

Presentation

Mr. Emmanuel Agah
Lead, Law Enforcement Laison Unit, CSA

Mr. Emmanuel Agah, in a presentation, outlined the core values of the CSA and its mandate. He spoke on the role of the "Safer Digital Ghana" Programme noting that it is a continuous awareness programme focusing on cyber related issues. His presentation on the "Cyber Trends of Our Society" was to educate the representatives of the Civil Society Organisations to appreciate the severity of the impact of cybersecurity and cybercrime issues.

According to Mr. Agah, of the top fifteen most visited websites in Ghana; four were sports betting websites; three were social media sites, four were news sites, three were pornography websites, and one was an information website.

He further noted that the top five (5) Cybersecurity Incidents received by the Cybersecurity/Cybercrime Incidents Reporting Points of Contact are as follows:



i. Online Fraud (Investment Scam, Romance Scam, Recruitment Scam) – 30%
ii. Unauthorised Access (Account Takeover, Phishing) – 30%
iii. Online Blackmail (Sextortion, Extortion) – 20%
iv. Online Impersonation (VVIP, High-Profile Personalities, Renowned Brands/Organisations – 5%
v. Publication of Non-Consensual Intimate Images (PNCII) – 3% and other cybersecurity incidents observed which was Information Disclosure, Online Child Sexual Exploitation & Abuse, Ransomware, DDoS, Malware, etc. – 12%

Roundtable Discussion

At a roundtable discussion, moderated by Ms. Afua Brown-Eyeson of the CSA, participants were given the opportunity to discuss issues and to devise solutions for the betterment of their organisations.

In this session, the participants urged the Authority to publicise the statistics on cybercrimes regularly and intensify awareness creation to help the public appreciate the urgency for the cybersecurity development. They also recommended carrying out educative exercises in local languages and pledged to work at improving cybersecurity in their organisations.

The Deputy Minister for Communications and Digitalisation reiterated that the Ministry and the CSA are committed to creating awareness and building capacity on various fronts. She urged the CSOs to collaborate with the CSA to ensure every Ghanaian appreciates and practices cyber hygiene.



Closing Remarks

Mr. Alexander Oppong
Lead, Capacity Building and Awareness Creation, CSA

Mr. Alexander Oppong expressed his gratitude to all for their active participation in the Forum. He reiterated that the partnership with CSOs is vital to the Cyber Security Authority and as part of its efforts in fulfilling its mandate. He informed the participants that the CSA has confidence in their ability to create the needed awareness on the potential online dangers that their members are exposed to and how the public can also protect themselves from becoming victims.

Mr. Oppong drew the attention of the participants to some of Government's initiatives towards securing the cyberspace, which include: the ratification of international conventions like the Budapest and Malabo Conventions, the passage of the Cybersecurity Act, 2020 (Act 1038), and establishment of the Cybersecurity/Cybercrime Incident Reporting Points of Contact (PoC) for reporting incidents and receiving advisories. He emphasised however that, the ultimate responsibility to remain safe and secure online lies at the doorstep of individuals and organisations.

Bank Boards and Executive Directors Briefing on "Ghana's Cybersecurity Act, 2020 (Act 1038); the Bank of Ghana Cyber and Information Security Directive; It's Implications and the Role of Board of Directors."

NATIONAL
CYBER SECURITY
AWARENESS MONTH

BANK BOARDS AND EXECUTIVE DIRECTORS BRIEFING ON "GHANA'S CYBERSECURITY ACT, 2020 (ACT 1038); THE BANK OF GHANA CYBER AND INFORMATION SECURITY DIRECTIVE; IT'S IMPLICATIONS AND THE ROLE OF BOARD OF DIRECTORS."



Background

The Cyber Security Authority (CSA) in collaboration with the Ghana Association of Banks (GAB) held an interactive breakfast meeting with Board Members and Directors within the financial sector in Accra. The program gave insight to and improved the awareness of the Cybersecurity Act, 2020, at the leadership level of Banks by discussing its implementation and implications on the financial sector and encouraged networking amongst the participants.



Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation

Remarks

Hon. Ama Pomaa Boateng
Deputy Minister for Communications & Digitalisation

Addressing the Board members and Directors of the various financial institutions that attended, the Deputy Minister for Communications and Digitalisation, Hon. Ama Pomaa Boateng, noted that the financial sector is at a high risk of cyberattacks and to mitigate these potential

cyber threats and risks to the industry, various regulatory compliance measures have been put in place; namely, the Cyber and Information Security Directive for financial institutions issued by the Bank of Ghana, the Critical Information Infrastructure Directive launched in October last year, and the Cybersecurity Act, 2020 (Act 1038). She noted that compliance with these measures will help improve cyber resilience in the financial sector.

She emphasised that the responsibility of ensuring that their respective organisations have sustainable digitalisation efforts lies in the hands of business leaders, directors, and CEOs. She encouraged the audience to adhere to the World Economic Forum's Principles for Board Governance of Cyber Risk which advises Board of Directors to align cyber risk management with business needs across every facet of decision-making, including innovation, mergers and acquisitions, product development and more.

Remarks

Dr. Maxwell Opoku-Afari
First Deputy Governor, Bank of Ghana

Representing the First Deputy Governor of the Bank of Ghana, Mr. Ismail Adam, Deputy Head of



Mr. Ismail Adam
Deputy Head of Banking Supervision,
Bank of Ghana



Banking Supervision of the Bank of Ghana, recapitulated that even though internet and modern technologies have been beneficial, they also expose financial organisations to several risks. Therefore, the questions leaders should be asking is "How can we benefit from the use of modern technologies with less risks?" He mentioned the Bank of Ghana's Cyber and Information Security Directive, 2018, stating that it seeks to provide a framework for establishing Cyber and Information Security protocols and procedures to the adoption of appropriate technologies and procedures to mitigate risk.

Mr. Ismail Adam shed light on the several initiatives the Bank of Ghana has provided to secure the operations and security of banks while ensuring the resilience and robustness of banking and financial systems. He announced that the Bank of Ghana has embarked on establishing a Financial Industry Command Security Operation Centre (FICSOC) to ensure better monitoring of digital systems.

He also noted that Banks should verify that staff who handle cyber-related issues have verified qualifications, as specified in the Directive. He further noted that various technological advances such as Blockchain engineering, Artificial intelligence and Machine learning are changing the financial sector and encouraged Board members to make provisions for these changes.

Welcome Remarks

Mrs. Mansa Nettey
President, Ghana Association of Banks

In welcoming the guests to the event, Mrs. Mansa Nettey said the meeting to deliberate on the Cybersecurity Act, 2020 (Act 1038) and other Directives and their implications was necessary as it provided Directors and CEO of banks the opportunity to learn more and adopt best practices. She noted that the increase of attacks on Critical Information Infrastructure affects various aspects of the nation, and could impede the adoption of digital financial services, retard



economic activities, generate substantial financial losses, undermine public confidence in emerging technologies, and cause major financial instability in the economy. Therefore, it is of utmost importance for the leadership of financial institutions to know how they can effectively implement cybersecurity measures within their respective organisations.

She encouraged participants to strategically partner with the Bank of Ghana and the Cyber Security Authority for effective implementation of the Cybersecurity Act, 2020tt (Act 1038), and for carrying out capacity building initiatives.

Presentation

THE CYBERSECURITY ACT, 2020 (ACT 1038)
Mr. Benjamin Ofori
Lead, Critical Information Infrastructure Protection, CSA

Mr. Benjamin Ofori, educated the audience on the Cybersecurity Act, 2020 (Act 1038). He cited recent cyberattacks targeted at the financial sector of countries such as Taiwan and Zambia. He indicated that the financial sector is part of Ghana's Critical Information Infrastructure (CII) in accordance with Sections 35-40 of Act 1038. He elaborated on Section 35, which provides for the designation of Critical Information



Infrastructure, stating that the Directive for the Protection of Critical Information Infrastructure establishes the baseline cybersecurity requirements for all designated CII owners, and must be complied with.

Presentation

THE BANK OF GHANA CYBER AND INFORMATION SECURITY DIRECTIVE, 2018

Dr. Samuel Senyo Okae
Bank of Ghana

Using the case of the American bank, JP Morgan's 2014 cyberattack where households, businesses, and customers emails were affected; Dr. Samuel Senyo Okae, the Information Security Office Head of the Bank of Ghana, noted the need for financial institutions



to be alert and be prepared for cyberattacks. He elaborated that JP Morgan's cyberattack caused the organisation to reconsider its cybersecurity policies and the need to pay more attention to this area of its operations.

By following the provisions of the Bank of Ghana's Cyber and Information Security Directive, Heads of Banks and other financial institutions would be sure to adopt and implement the right cybersecurity measures. Dr. Okae highlighted the key areas Directors should note within the Directive, particularly the respective roles and expectations of the Board and Senior Management in ensuring that their organisations are prepared for cyber threats or attacks. He emphasised that Management and



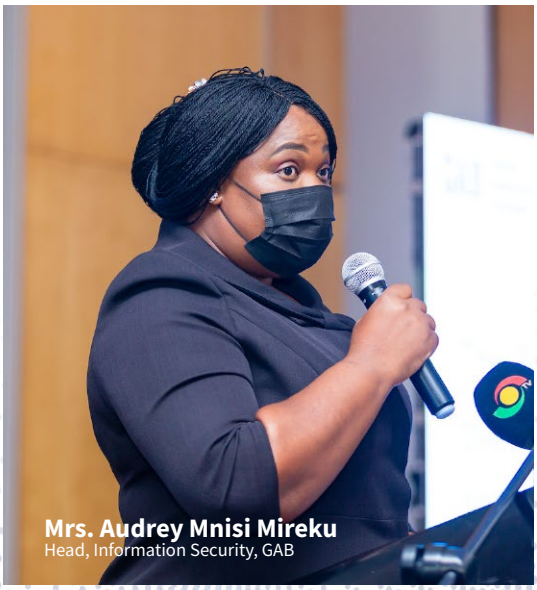
Boards should ensure effective internal controls and risk management practices are implemented correctly.

Presentation

THE ROLE OF BOARD DIRECTORS IN THE IMPLEMENTATION OF GHANA'S CYBER REGULATIONS

Mrs. Audrey Mnisi Mireku
Head, Information Security, GAB

Mrs. Audrey Mireku's presentation on "The Role of Board Directors in the Implementation of





Ghana's Cyber Regulations," enumerated challenges and threats the financial sector faces in respect to cybersecurity, which include a lack of cybersecurity skills at the Senior Management Level, overregulation, lack of appropriate budget, and talent gaps. She shed light on cyberattack threats commonly experienced by banks. These are data breaches, ransomware attacks, insider threats, complex supply chain ecosystem, and social engineering.

According to Mrs. Mireku, these attacks and threats negatively impact organisations such as the loss of critical data, operational downtime, unauthorised disclosure, and service disruption. On this note, she urged the Board of Banks and other financial institutions to be proactive concerning their role in improving cybersecurity development within their organisation. She emphasised that the Board has the role of growing expertise within the organisation, developing positive cybersecurity culture, and understanding the cyber threats, risks, and vulnerabilities, to implement effective risk management policies and cybersecurity measures.

Conclusion and Recommendations

At the end of the section, the following recommendations were made:

i. Information sharing amongst financial Institutions must be improved to effectively tackle cybersecurity related issues.
ii. Business leaders should consider career guidance and professional development programs towards developing their cybersecurity posture.
iii. Financial institutions should intensify awareness creation on cyber risks and promote appropriate incident reporting and response practices such as the establishments of Computer Emergency Response Teams (CERTs).
iv. Financial CII owners were urged to maximise their effort in complying with the CII registration processes.

The event ended with closing remarks from the CEO of the Ghana Association of Banks, Mr. John Awuah. He thanked the participants and guests for being a part of the event and encouraged them to be intentional in their efforts towards securing their organisations digital assets and processes.

Technical Training for Personnel of the CSA and Other Joint Cybersecurity Committee Institutions



NATIONAL
CYBER SECURITY
AWARENESS MONTH

TECHNICAL TRAINING FOR PERSONNEL OF THE CSA AND OTHER JOINT CYBERSECURITY COMMITTEE INSTITUTIONS



Background

The Cyber Security Authority (CSA) as part of activities marking the 2022 edition of the National Cyber Security Awareness Month (NCSAM), in partnership with Huawei S.A. Technologies, Ghana organised a two-day technical training for forty (40) participants selected from the CSA and the Joint Cybersecurity Committee institutions including the National Communications Authority (NCA), National Information Technology Agency (NITA), Data Protection Commission (DPC), Bank of Ghana (BoG), Financial Intelligence Centre (FIC), Economic and Organised Crime Office (EOCO), Criminal Investigations Department (CID), National Security (NS), Defense Intelligence (DI), Research and Development(RD), National Signals Bureau (NSB), Ghana Immigration Service (GIS), Ghana Armed Forces (GAF), Office of the Attorney General (AG), Judicial Service of Ghana (JS) National Intelligence Bureau (NIB), Energy Commission (EC), and the Ghana Domain Name Registry (GDNR).

Opening Remarks

Zhoujianling Jenny
Senior Manager
Huawei S.A. Technologies, Ghana

Madam Zhoujianling Jenny, on behalf of her team welcomed all participants to the training. She added that she and her team were excited to be a part of this year's National Cyber Security Awareness Month (NCSAM). She acknowledged that Ghana has made some remarkable strides in the cybersecurity ecosystem and that Huawei S.A. Technologies were happy to contribute their quota towards the development of cybersecurity in the country.

Day1

INTERNATIONAL CYBERSECURITY STANDARDS AND THREAT INTELLIGENCE GATHERING

The trainers for the day were Robin Wang and Jipeng Liu. Robin Wang took participants through two widely used international cybersecurity standards, the ISO 27001, and the Network Equipment Security Assurance Scheme (NESAS SCAS) while Jipeng Liu handled the training on threat intelligence gathering.

Mr. Robin Wang in his presentation emphasised the need for standards. He stated that international standards helped the world speak a common language, he gave an example of the Greenwich Meridian Time (GMT) which is a world-wide accepted way of measuring time. He explained that a standard which is a widely agreed way of doing something had many benefits including allowing room for interoperability and avoiding duplication of effort. He went on to address the fact that, the more we relied on digital systems, the more vulnerable we become and hence imploring the use of security standards, policies and guidelines were very crucial as it helped to reduce risk drastically.

Mr. Robin Wang mentioned that security standards could be classified in three domains. The first one was viewed from the player perspective i.e the international, regional, national, industry and corporate standards. The second classification looks at the function domain i.e security governance, risk management, audit, vulnerability management, certification etc. The third classification was by industry domains such as wireless security, privacy protection, cloud security, security governance etc.





The International Organisation of Standards (ISO) is an independent, non-governmental organisation with a membership of 165 national standards bodies. Through its members, it brings together experts to share knowledge and develop market relevant international standards that support innovation and provide solutions to global challenges. Focusing on the ISO 27001 standard, Mr. Robin Wang explained that this standard was highly relevant in the information security management system (ISMS). The objective of the ISO 27001 is to establish, implement and continuously improve the information security management system. It was worth noting that at the core of any ISMS was leadership and that for the successful implementation of an ISMS, the leaders of an organisation needed to buy into the idea of information security. ISMS builds confidence and trust and provides a high level of security assurance.

The Network Equipment Security Assurance Scheme and the Security Assurance Specifications (NESAS SCAS) standard was also another standard, participants were taken through. The NESAS SCAS is a collective work by the Global System for Mobile Communication Association (GSMA) and the 3rd Generation Partnership Project (3GPP), which acts as a

mobile industry-wide network security evaluation framework. It is relevant to carriers, vendors, regulators, and industry partners. The unified design of the evaluation process helps to prevent conflicting security assurance requirements in different markets. This standard also shows evidence of collaborative work among industry players.

Moving on to the second session of the day, Mr. Jipeng Liu took participants through Cybersecurity Threat Intelligence (CTI) Gathering. Threat intelligence focuses on evidence-based knowledge. The essence of performing threat intelligence is to enable organisations make faster and more informed security decisions. It also encourages a more proactive behaviour in the fight against cyber-attacks. Participants gained knowledge on how to launch a CTI project as well as build and operate threat intelligence platforms. They were also introduced to new and existing tools such as MISP as well as to the different CTI communities which could aid in threat intelligence programs.

Day2

INCIDENT HANDLING & COMMUNICATION AND CYBERSECURITY INCIDENT RESPONSE STANDARDS AND FRAMEWORKS

Mr. Martin Lie, the instructor for the second day took participants through three widely used standards for computer emergency response which are:

i. NIST SP800-61-2 Computer Security Incident Handling guide,
ii. Gartner Cybersecurity Incident Response Plan (CIRP),
iii. NCSC (UK) Cyber Incident Response Guidance (CIRG).

It was important to note that, all the above-mentioned models were similar to the Prepare, Detect, Contain, Eradicate, Recovery



and Follow up (PDCERF) incident handling model. While the NCSC (UK) Cyber Incident Response Guidance (CIRG) was more tailored to regulators, the NIST framework provides references for enterprises such as Cybersecurity Service Providers (CSPs) to build incident response. The US government agencies and their suppliers are also required to comply with NIST standards. The Gartner cybersecurity incident response plan (CIRP) was more suitable for small-scale and large-scale enterprises as it provides them the necessary tools and templates to be used as reference for building a cybersecurity incident response system.

Conclusion

At the end of the training participants gained comprehensive knowledge on international cybersecurity standards, cybersecurity threat intelligence gathering, incident handling and communication, and cybersecurity incident Response Standards and Frameworks. They were awarded with certificates for undergoing the training. Participants were taken to Aqua Safari Resort in Ada for a one-day retreat after the training.

Stakeholder Related NCSAM 2022 Events

NATIONAL
CYBER SECURITY
AWARENESS MONTH

INAUGURATION OF EMANOR YOUTH IN CYBERSECURITY

Emanor Cyber Security, a private cybersecurity company that is targeted at the youth from the Zongo communities of Ghana in a bid to reduce unemployment and cybercrime in Zongo communities, by equipping them with essential IT skills, invited the CSA to partake in the company launch under the theme: "Zongo Youths in Cyber Security, The Time is Now". Resource persons from the CSA were Mr. Eric Kafui Bansah, Deputy Manager of the Capacity Building and Awareness Creation (CBAC) Functional Area and Mr. Godfred Kumi Kwakye, Deputy Manager of the IT Standards Functional Area.

Mr. Bansah in his presentation stated that digitalisation comes with a number of benefits which must be capitalised on for socio-economic development. He however cautioned that there are increasing risks in cyberspace and hence the need for the participants to know about such risks and to practice good cyber hygiene. He briefed the participants on Ghana's Cybersecurity Act, 2020 (Act 1038) and emphasising on sections 62-68 of the Act, urged them to restrain from child online abuses and non-consensual sharing of intimate images and videos of others.



Mr. Godfred Kumi Kwakye's presentation demonstrated some cybersecurity recommended best practices to the youth. He emphasised the importance of practicing cyber hygiene to be safe anytime one is using the internet. Mr. Kwakye advised the participants to develop strong passwords, use multifactor authentication and to routinely update software. He stated the dangers associated with interacting with strangers online and advised the participants to report any cyber related incidents to the CSA's Cybersecurity/Cybercrime Incident Reporting Points of Contact.

YOUTH WITHOUT BORDERS

Youth Without Borders, a Ghanaian youth organisation, organised a three-day online National Cyber Security Awareness workshop for their constituents who were about 100 in number.

The CSA was represented by Madam Patricia Adafienu, an Assistant Manager from the Capacity Building and Awareness Creation Functional Area (CBAC) of the CSA. She took the audience through a series of presentations which included the need to ensure a safe experience online. She introduced the participants to the prospects and opportunities in cybersecurity and urged them to take up careers in the profession.

The participants made a request to CSA to organise more awareness creation programmes to increase knowledge of cybersecurity matters among the people, and to also help publicise the Authority.

GENIUS INFORMATION & TECHNOLOGY FOUNDATION

The Genius Information & Technology Foundation (GITF) in collaboration with the Cyber Security Authority and Institute of ICT Professionals (IIPGH) Ghana held an open lecture to educate the public on the proper and effective ways to stay safe while using the internet. The event adopted the hybrid approach with about 100 participants.

Mr. Isaac Socrates Mensah, a Deputy Manager of the Computer Emergency Response Team (CERT) of the Cyber Security Authority (CSA) made a presentation on cybersecurity development initiatives in Ghana indicating that cybersecurity issues are more of a social problem than a technical problem. He added that the internet is a global village where anything can be shared at any time by anyone and that there are laws which govern the day-to-day usage of the internet that the participants must be conversant with. He made reference to Sections 62-68 of the Cybersecurity Act, 2020 which focus majorly on the protection of children online and the fact that child online offences attract up to 25 year imprisonment.

CEIBS ALUMNI LECTURE

The webinar was organised by CEIBS Ghana Chapter as part of the National Cyber Security Awareness Month (NCSAM) 2022 by means of a virtual platform.

Mr. Alexander Oppong, Functional Lead for Capacity Building and Awareness Creation (CBAC) spoke at the webinar on the topic "Cybersecurity, What You Should Know", to about 29 Chief Executive Officers and Senior Officers of various institutions.

Mr. Oppong gave an overview of the CSA, including its mandates as stipulated in the Cyber Security Act, 2020 (Act 1038). He further educated the Chief Executive Officers and Senior Officers from the various organisations represented on the need to protect Critical Information Infrastructure, the CII directive, and the Computer Emergency Response Team (CERT) ecosystem.

Taking the participants through cybersecurity best practices, Mr. Oppong urged them to ensure proper governance systems by ensuring that user policies and guidelines are properly in place in their institutions; ensuring that there are technical control and compliance measures and the adoption of proper cybersecurity solutions. He also urged them to build the capacity of the staff in their institutions in cybersecurity.

Mr. Oppong advised the participants to create strong passwords, use multifactor authentication on their devices, beware of social engineering schemes and if possible, stay away from the use of public wi-fi.

ROLL BALL FEDERATION NATIONAL CHAMPIONSHIP

The Capacity Building and Awareness Creation (CBAC) and the Computer Emergency Response Team (CERT) Functional Areas of the Cyber Security Authority (CSA) honoured the invitation of the Roll Ball Federation and participated in the Roll Ball National Competition at the University of Ghana Campus.

In a presentation, Mr. Eric Bansah, Deputy Manager of the CBAC commenced his presentation by educating members of the Federation on the Cybersecurity Act, 2020 (Act 1038). He urged the sportsmen and women to be cyber conscious and said that cyber breaches are caused by human error at about 95% of the time. He added that the success of cyberattacks can cause severe socio-economic damages and urged them to use sports as a tool to create cybersecurity awareness among their colleagues and fans.

Mr. Antwi Attoh, an Assistant Manager of the CERT in his presentation, stressed on the importance of good cyber hygiene practices and urged participants to avoid sharing their passwords with others, generate strong passwords and update softwares regularly. He then sensitised them on Social Media Impersonation. They were also advised to reject unsolicited calls, emails and text messages, especially from unknown contacts since they could be cyber fraudsters.



Mr. Antwi Attoh concluded by informing the participants about the CSA's Cybercrime/cybersecurity Incident Reporting Points of Contact (PoC) and urged them to report all cyber related occurrences to the CSA.



ENTREPRENEURSHIP SUMMIT 2022

This was a summit organised by The Methodist Church of Ghana, Northern Diocese, Dome Circuit on the theme, "***Making the best out of social media***". The Cyber Security Authority honoured their invitation to speak to participants on how to stay safe online when using social media.

The officials of the CSA led participants through cybersecurity best practices that will help them to protect themselves and their businesses online. Some of these include keeping personal information private, keeping passwords secured, and using debit and credit cards responsibly while conducting online transactions.

TELECOMS CHAMBER EDUCATES ABOUT 2000 STUDENTS, TEACHERS AND PARENTS ON CYBERSECURITY

Background

The Ghana Chamber of Telecommunications in collaboration with the Cyber Security Authority (CSA) educated about 2000 students, teachers and parents within the La-Dadekotopon Municipal Assembly in Accra.
The educational exercises, which formed part of the 2022 National Cyber Security Awareness Month, were carried out in 2 different schools in the Greater Accra region.

The first engagement took place at St. Thomas Aquinas SHS on October 19, 2022. About 1,500 students from SHS 1 and SHS 2 along with their teachers were taken through key topics such as "***The Reality Of Cybercrime On Social Media***", "***The Consequences Of Engaging In Cybercrime***" and "***Steps To Take To Protect One's Self Online***".

The sessions were handled by experts from the Cyber Security Authority, AirtelTigo Ghana, Vodafone Ghana and MTN Ghana. There was an interactive question and answer time, as well as the gifting of numerous prizes and souvenirs to the students and their teachers.

Remarks

Dr. Ing. Kenneth Ashigbey
CEO, Ghana Chamber of Telecommunication

Taking his turn to address the students, the CEO of the Ghana Chamber of Telecommunications, Ing. Dr. Kenneth Ashigbey, charged the students to take advantage of the numerous opportunities presented by the digital platforms around them and also take steps to protect themselves.

The second engagement took place at the Labone SDA School on October 21, 2022 on the theme: "Digital Parenting Forum on Child Online Protection". Parents of students of the school who were the target for the engagement were taken through different topics bordering on "how parents can protect themselves, their businesses and their children online".
The facilitators, who were officials of AirtelTigo Ghana, MTN Ghana and Vodafone Ghana, reiterated the need for parents to exercise extreme care in the information they put online, the people they interact with online and the liberties they give their children when it comes to their use of digital devices and the content they consume.



CSA ENGAGES MEMBERS OF THE TELECOMMUNICATIONS CHAMBER FOR EFFECTIVE CYBERSECURITY REGULATIONS



Background

Ghana's Cybersecurity Act, 2020 (Act 1038) provides the legal basis for multi-stakeholder engagements for effective collaborations and partnerships for the country's cybersecurity development. As part of measures to effectively implement Act 1038, the Cyber Security Authority (CSA) leveraged on the 2022 edition of the annual National Cyber Security Awareness Month (NCSAM) to partner with the National Communications Authority and the Ghana Chamber of Telecommunications to engage members of the Chamber of Telecommunications. A breakfast meeting was held to provide a forum to engage with relevant stakeholders in the telecommunications industry to deliberate on current issues including the protection of the telecommunications sector as a designated Critical Information Infrastructure (CII) sector.

Remarks

Dr. Albert Antwi-Boasiako
Ag. Director General, CSA



According to Dr. Antwi-Boasiako, Ghana's digital infrastructure depends largely on the telecommunications sector and as such there is the need to work together by engaging in regular dialogues and debates. This, he said, will help identify common grounds that will ensure a secure and resilient digital ecosystem. He said, "we have one goal; ensuring a safer digital environment, but we have differentiated responsibilities and mandates as individuals and institutions to achieve the goal".

He cited Sections 35-40 of Act 1038, which focus on the designation of Critical Information Infrastructure (CII), registration of the owners of CII and the duties of these CII owners. He added that the CSA is committed to working with the telecommunications sector in the implementation of Section 69 of the Act in collecting relevant subscriber information for investigation purposes when required. He further encouraged them to take interest in the establishment of the Industry Forum per section 81 of the Cybersecurity Act, 2020.

Dr. Antwi-Boasiako indicated further that, the licensing and accreditation regime for Cybersecurity Service Providers, Cybersecurity Establishments and Cybersecurity Professionals will be implemented from January 2023. He thus encouraged the participants to embrace the regulations as they are very necessary considering the intrusive nature of cybersecurity activities.

Remarks

Dr. Ing. Kenneth Ashigbey
CEO, Ghana Chamber of Telecommunication



Ing. Dr. Kenneth Ashigbey in a presentation indicated key issues that the industry was facing. Notable among them were loss of lives, fibre cuts, theft of telecom equipment & resources including batteries, fuel, fire extinguishers etc.

Remarks

Professor Ing. Yeboah Boateng
Deputy Director-General (Technical Operations), NCA



Speaking at the event, Professor Ing. Ezer Yeboah Boateng, representing the Director-General of NCA, said there were a number of cybersecurity issues affecting the industry with respect to Availability, Confidentiality and Integrity of the operations of the telecommunications sector. He said the forum was therefore apt; an opportunity to highlight challenges facing industry players and to set in motion frameworks to safeguard the telecommunications ecosystem. He said, NCA is committed to continuous engagements with the CSA and the industry players through the Telecommunications Sector Computer Emergency Response Team (CERT) for a sustained digital transformation.

International Cooperation Related Events

NATIONAL
CYBER SECURITY
AWARENESS MONTH

INTRODUCTORY TRAINING COURSE ON CYBERCRIME FOR JUDGES AND PROSECUTORS



Background

The Economic Community of West African States (ECOWAS) Commission and the Council of Europe (CoE), in collaboration with the Cyber Security Authority (CSA), partnered through the Global Action on Cybercrime Extended (GLACY+) and the West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR-C) Projects to organise a 4-day introductory training course on cybercrime for Judges and prosecutors and training of trainers. This introductory training course sought to equip participants to prosecute and adjudicate cybercrime cases, make use of electronic evidence, and become trainers on these matters.

The training was attended by representatives of the Judicial Service of Ghana, Office of the Special Prosecutor, Attorney General's Department and Ministry of Justice, Criminal Investigations Department of the Ghana Police Service, Economic and Organised Crime Office and the Cyber Security Authority.

Day 1

Welcome Address

Dr. Albert Antwi-Boasiako
Ag. Director-General, CSA

Dr. Antwi-Boasiako commenced his remarks by expressing his appreciation on behalf of the Cyber Security Authority to the international partners and the participants present at the training. He stated in his delivery that, the training programme was designed to develop and build upon existing capacity to then support the state to deliver training to several people. He indicated that law enforcement officials should be first responders to cybercrime handling by appreciating electronic evidence because regardless of expertise, certain district officers are likely to find a computer system or a device at crime scenes and responders are required to be qualified to handle that. He added that the training programme was important because for judges, especially, to effectively adjudicate matters of such nature, they must understand the best practice approach to respond to incidents before exhibits are transported to forensics labs for analysis to support the various court processes.

Remarks

Ms. Catalina Stroe
Project Manager, GLACY+ Project

Ms. Catalina Stroe indicated that the training course is not only for Ghana, but for the entire ECOWAS region and Mauritania. She emphasised that since Ghana has a robust response to cybercrime, there was the need for Ghana to have a leading role in nurturing the capacities of the rest of the ECOWAS member states.

Ms. Stroe Catalina explained that the training is under the Global Action on Cybercrime Extended (GLACY+) Project, co-funded by the European Union and Council of Europe running since 2016. Adding that, they are part of a bigger family called the Cybercrime Programme Office, based in Bucharest. She revealed that one pillar; the GLACY+ Project was to build upon and to strengthen the capacities of prosecutors, investigation units and criminal justice offices in collaboration with Interpol.

With regards to the training for judges, she indicated that they work with national authorities and judicial training institutions in streamlining the national training structures and the build-up of a network of judicial trainers to facilitate the training of trainers within a country or region.



"We want to have a guideline on judicial training strategies; hence we are looking to have a draft of this guidebook by late 2023 to be able to present it in the plenary session next year", she added.

She further expressed the hope that participants would become knowledgeable and fully capable to offer trainings to their peers after the end of the course.

Remarks

Hein Dries
Key Expert, OCWAR-C PROJECT

Mr. Hein Dries expressed his appreciation to Dr. Albert Antwi-Boasiako, the Director-General of the CSA and noted that the team will look at holding a residential training next year. He further stated that the objectives of the West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR-C) Project is to contribute to enhancing cybersecurity and the fight against cybercrime in the ECOWAS region and in the Islamic Republic of Mauritania. He added that the Malabo Convention has recently been ratified by The Gambia. He however noted that, the ratification of the Budapest Convention has been more successful compared to the Malabo Convention.

TRAINING ON INTERNET BASICS FOR JUDGES AND PROSECUTORS

This session was facilitated by Mr. Jacob Puplampu (A Trainer-of-Trainers for the Council of Europe). In his presentation, he addressed computer parts and functions, internet parts and how they came to be, connecting to the internet, internet services and applications, deep web, anonymity, and the dark web. This session enabled participants to recognise the common components of a computer system and understand their role. It also described what the internet is, how someone connects to it and

what possible traces can be left in the process in doing so. The session also enabled participants to list some internet services and applications they encounter in their daily roles as prosecutors, judges and law enforcement officers such as Peer to Peer networks which allow users to offer files for sharing and search for files by name, type, artist or author and on which many illegal files are present. Issues the dark web can bring to criminal prosecutions as well as cryptocurrency were also addressed.

Training on Cybercrime Basics (An Introduction to Cybercrime)
This session was facilitated by Mr. Branko Stamenkovic (a GLACY+ Project Expert) and provided participants with an introduction to the information society and cybercrime and efforts to tackle this modern type of criminality by international organisations such as the United Nations, Council of Europe, African Union, INTERPOL, among others. This session further provided basic definitions of cybercrime and defined contemporary forms of cybercrime such as cryptocurrency, cloud attacks, payment fraud such as skimming, shimming and jackpotting, child sexual exploitation, among others. Additionally, the needs and the advantages of the harmonisation between national legislation and international instruments, particularly the Budapest Convention were addressed.

Day 2

THE MALABO CONVENTION AND THE ECOWAS DIRECTIVE

This session was facilitated by Ms. Jennifer Mensah (a Trainer-of-Trainers for the Council of Europe). She addressed the scope and reach of the Malabo Convention and the ECOWAS Directive on Fighting Cybercrime, noting that the Malabo Convention was adopted by the African Union on June 27, 2014, whereas the ECOWAS Directive was adopted in August 2011.



She further stated that the Malabo Convention has sections on the protection of personal data and privacy, the promotion of cybersecurity and combating cybercrime, and the security of electronic evidence. Additionally, she noted that the scope of the cybercrime section of the Malabo Convention and the scope of the ECOWAS Directive included substantive law, sanctions and procedural law. Ms. Mensah highlighted that both the Malabo Convention and ECOWAS Directive have provisions on international cooperation, even though they are non-binding, and called on member states to make use of existing international instruments to enhance international cooperation. Currently, 14 member states have signed the Malabo Convention. Ghana signed the Malabo Convention on July 14, 2017, and ratified the Convention on May 13, 2019.

THE BUDAPEST CONVENTION

This session which was also facilitated by Ms. Jennifer Mensah (a Trainer-of-Trainers for the Council of Europe). She addressed the scope and reach of the Budapest Convention, the fundamentals of a cybercrime treaty and the benefits of the Budapest Convention. Ms. Mensah stated that the three pillars of the Budapest Convention were Criminalising



Conduct, Procedural Tools and International Cooperation. She added that the Budapest Convention is for the protection of the rights and interests of people in cyberspace and the approach by the Council of Europe to achieve this includes common standards, the T-CY Committee of which Ghana is a member and has the responsibility to conduct assessments of the implementation of the provisions of the Budapest Convention, and Capacity Building. Some benefits of the Budapest Convention mentioned included improvements to domestic legislations, enhancement in the total number of investigations into cybercrime being conducted, and extensive use of 24/7 networks, among others. Ghana acceded to the Budapest Convention on December 3, 2018.

Part 1

TRAINING ON SUBSTANTIVE PROVISIONS OF THE BUDAPEST CONVENTION

This session which was facilitated by Ms. Jennifer Mensah (a Trainer-of-Trainers for the Council of Europe) provided participants with a comprehensive understanding of the elements of offences against the confidentiality, integrity and availability of computer systems and data, established in accordance with the Budapest Convention. Additionally, fundamental terms such as computer data, computer system, traffic data and service provider were defined as well as elements which constitute the offence of illegal access, illegal interception, system interference, misuse of devices and data interference.

Part 2

TRAINING ON SUBSTANTIVE PROVISIONS OF THE BUDAPEST CONVENTION

Facilitated by Mr. Branko Stamenkovic (a GLACY+ Project Expert), this session addressed computer-related forgery noting that the scope of this offence is limited to the falsification of documents by the input of correct or incorrect data, subsequent alterations, deletion, and suppression. He also addressed the issue of computer-related fraud provided for in Article 8 of the Budapest Convention and addressed Child Pornography which is addressed in Article 9 of the Budapest Convention where he explained the terms “without rights”, “pornographic materials”, “minor”, among others.

Training on Procedural Powers under the Budapest Convention

This session was facilitated by Mr. Matteo Lucchetti (an OCWAR-C expert) who explained that Article 15 of the Budapest Convention provides for the establishment, implementation and application of the powers and procedures stated in the Budapest Convention. He further addressed the procedural powers covered in the Budapest Convention namely expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, among others. On the expedited preservation of stored computer data, participants raised concerns regarding the reluctance of telecommunication companies to release information such as IP addresses to help in the investigation of cybercrime. It was recommended that the Cyber Security Authority

facilitates conversation with the telecommunication sector to address these issues.

Day 3

TRAINING ON BEST PRACTICES IN CYBERCRIME PROSECUTIONS

This session which was moderated by Madam Yvonne Atakora Obuobisa (a Trainer-of-Trainers for the Council of Europe) addressed the best evidence in the prosecution of cybercrime, the use of electronic evidence, admissibility of electronic evidence, and human rights safeguards in cybercrime trials. She further noted that if handled properly, electronic evidence is one of the best types of evidence for the prosecution of cybercrime for various reasons including the fact that IP addresses in emails can sometimes be checked. Regarding Ghana's position on electronic evidence, she stated that the country's law distinguishes criminal law procedure from civil matters.

At the end of this session, suggestions and comments were made regarding CSA's role in facilitating conversations and deliberations with the telecommunication sector to solve the problem of reluctance on the part of telecommunication companies to release information such as IP addresses to aid in cybercrime investigations, as well as, the suggestion for an amendment to the Cybersecurity Act, 2020 (Act 1038) with regard to Sections 69 to 74 which make reference to cybersecurity and investigatory powers, where the application for production order and interception warrant is limited to the High Court and should be expanded to the lower courts as time is of the essence in cybercrime investigations.

Basic Concepts on International Cooperation

This session which was moderated by Mr. Branko Stamenkovic (a GLACY+ Project Expert) enabled participants to understand the global dimension of the Internet and the international dimensions of cybercrime, the challenges of cybercrime in the international environment, the importance of international cooperation and recognising the available instruments for international cooperation in the field of cybercrime. The session also identified the general and special principles and articles on Mutual Legal Assistance (MLA) in criminal matters.



ELECTRONIC EVIDENCE AND INTRODUCTION TO DIGITAL FORENSICS

This session which was moderated by Mr. Jacob Puplampu (a Trainer-of-Trainers for the Council of Europe) addressed the various types of electronic evidence, summarised key points from the Council of Europe Electronic Evidence Guide especially the principles of seizure and handling, identified differing challenges of "dead box" and "live data" forensics as well as "cloud-based data." Mr. Puplampu further explained the admissibility of electronic evidence and compared "digital forensics" to "traditional forensics". Lastly, he highlighted the four principles of electronic evidence namely data integrity, audit trail, specialist support and appropriate training.

Day 4

CYBERCRIME LEGISLATION (NATIONAL LEGISLATION)

This session was facilitated by Madam Yvonne Atakora Obuobisa (a Trainer-of-Trainers for the Council of Europe) and addressed the provisions of Ghana's Cybersecurity Act, 2020 (Act 1038) relative to substantive provisions, including child online protection, procedural provisions and evidential issues that may arise during investigations and trials.

Regarding the issue of admissibility of evidence, especially where there is a question on a breach of privacy rights, she stated that the Judge may have to take a decision in light of RAPHAEL CUBAGEE v. MICHAEL YEBOAH ASARE (Suit No. J6/04/2017 dated February 28, 2018), where the Supreme Court distinguished between the treatment of digital evidence in civil proceedings as against criminal matters and, in conclusion, adopted for Ghana the discretionary rule for the exclusion of evidence obtained in violation of human rights guaranteed under the 1992 Constitution.

Remarks

Madam Afua Brown-Eyeso
Lead, Child Online Protection Cyber Security Authority

Madam Afua Brown-Eyeson delivered the closing remarks on behalf of the Director-General of the CSA. In her remarks, she expressed her appreciation to the ECOWAS Commission, OCWAR-C, and the Council of Europe for organising this training course in Accra through GLACY+ Project. She expressed appreciation to all facilitators and assured participants that the CSA is not relenting in its efforts to fight cybercrime and will remain resilient, determined, and focused with the view to achieving its mandate to regulate cybersecurity in Ghana and to promote the development of cybersecurity in the country.

Closing Remarks

Madam Anna Lixi
European Union Delegation Representative

Madam Anna Lixi addressed the work of the European Union (EU) in general and its work in Ghana, highlighting that the EU works with Judges and Prosecutors within the framework of many projects and finances some activities of prosecutors beyond the Office of the Special Prosecutor, including the provision of digital equipment to the Ghana Police Service. She further stated that the EU always integrates digital tools in their various programmes and highlighted the importance of paying attention to the issues of cybersecurity.

Conclusion

In conclusion, there was a pre-survey and post-survey conducted on participants. Overall feedback indicated that the training was successful, and the participants acquired knowledge and skills in cybercrime and electronic evidence which will be beneficial to their jobs.

GHANA'S PARTICIPATION IN THE 7TH SINGAPORE INTERNATIONAL CYBER WEEK (SICW)

Background

The Singapore International Cyber Week (SICW) is Asia-Pacific's most established cybersecurity event which brings together global policymakers, industry leaders, and top academia across the world to exchange best practices and strengthen international cooperation on topics ranging from emerging digital opportunities and cyber threats, the evolution of cyberspace and cybersecurity policies, implementation of cyber norms, Internet of Things (IoT) and Operational Technology (OT) security. The event is organised by the Cyber Security Agency of Singapore (CSA), Singapore's national authority for cybersecurity which plays a pivotal role in Singapore's Smart Nation and digital economy ambitions.

The 7th Singapore International Cyber Week (SICW) took place in Singapore from October 18 to 20, 2022 on the theme, "Digital Security: A Shared Responsibility" and was in line with the theme for Ghana's National Cybersecurity Awareness Month (NCSAM), Regulating Cybersecurity, a Public-Private Sector Collaborative Approach.

The 2022 SICW was organised with a focus on the need to drive the momentum on cyber capacity building and international partnerships amid growing cyber threats and evolving strategies to mitigate the volatile relations between state and non-state actors.

Remarks

In his opening remarks, the Chief Executive of the Cyber Security Agency of Singapore (CSA) Mr. David Koh, posited that Cyber-attacks do not respect national boundaries, "just as states grapple with the cyber-related spill over effects from global conflicts, the landscape is also increasingly fraught with cyber threats which will only grow in frequency and complexity". As part of the country's team-effort strategy to tackle cyber threats, Mr. Koh announced plans





to build cyber talent capacity, as well as help emerging SMEs practice better cyber hygiene practices. He indicated that one of the key problems that the cybersecurity industry faces is the lack of cybersecurity talent in workforces across the globe. He expressed the concern that with the most advanced cyber technologies, organisations would remain largely vulnerable to cyberattacks without the right personnel to oversee and regulate them. This statement is significant because prior to the promulgation of the Cybersecurity Act, 2020 (Act 1038) and the establishment of the Cyber Security Authority (CSA), Ghana's cybersecurity sector was generally not regulated. The Government, through the CSA, is taking active steps to regulate the sector, build capacities and provide the enabling environment for the development of the right cybersecurity related talents to support the industry.

The Minister for Communications and Information and Minister in charge of Smart Nation and Cybersecurity, Mrs. Josephine Teo, encouraged nations to unite to build a sustainable digital future together.

Panel Discussions

A Ministerial Roundtable on "Cyber Resilience in the New Normal" explored the challenges of transboundary cyberspace, the importance of safeguarding nations' digital commons, and the critical need to ensure open communication channels in building trust in cyberspace.

The Speakers at the session included Brunei's Minister-in-charge of Cybersecurity, Pengiran Dato Paduka Haji Mustapha, New Zealand's Minister for the Digital Economy and Communications, Dr. David Clark, Philippines' Secretary of Information and Communications Technology, Ivan John Uy, and Ghana's Minister for Communications and Digitalisation, Hon. Mrs Ursula Owusu-Ekuful.

The panel emphasised the need for governments to work with industry to protect and enhance the resilience of cyberspace, indicating that combating cybercrime and malicious activities in cyberspace requires a multi-stakeholder approach with the roles and responsibilities of government agencies and other collaborating partners clearly defined. Highlighting Ghana's experiences in working with relevant stakeholders through the Joint Cybersecurity Committee and the Industry Forum established under the Cybersecurity Act,

2020 (Act 1038), Mrs. Owusu Ekuful stated further that the decentralised nature of Ghana's National Computer Emergency Response Team (CERT) is a key component of multi-stakeholder approach towards cybersecurity development.

In another development, a panel discussion on the Implications of Securing the Digital Future" agreed that the splintering of the internet is a complex and multi-faceted issue. As a result, Nation-states should first identify their topline cybersecurity risks and areas of concern as a basis for collaboration with international partners to harmonise and integrate the fragmented Internet. Discussions further focused on the need to continue improving cyber resilience, in order to tackle the ever-evolving cyber threats facing society. Panelists established that efforts will include upskilling people, as well as supporting innovation towards more robust processes and solutions that will be able to detect and respond to cyber incidents swiftly in the OT environment.

Bilateral Discussions

A bilateral discussion between Mrs. Josephine Teo and Mrs. Ursula Owusu agreed on deepening collaboration on cybersecurity cooperation in Critical Information Infrastructure Protection, cybersecurity skills development and experience sharing, regulation of Cybersecurity Service Providers, capacity building, and professional exchanges between the two countries. Mrs. Josephine Teo congratulated Ghana on her election to the International Telecommunications Union (ITU)'s Council at the ITU Plenipotentiary Conference in Bucharest, Romania, and expressed appreciation for Ghana's support for the United Nations-Singapore Cybersecurity Fellowship which Ghana is a participant.

Further discussions with representatives of INTERPOL's Global Complex for Innovation (IGCI), based in Singapore, touched on improving collaboration and support for Ghana's criminal justice sector through capacity building and assistance with investigations into cybercrimes and digital forensics capabilities.

Recommendations

- Digitalisation has become necessary for economic development, making developed and developing countries targets of ransomware actors. A "shared responsibility," is thus needed to combat cybercrime across developed and developing economies.
- Strengthening the global cybersecurity architecture requires a multi-stakeholder approach.
- A strong global cybersecurity architecture that gives people and businesses the confidence and trust to engage in the digital domain must be promoted.
- There is the need for unity among stakeholders to ensure cyberspace remains open, stable, and interoperable.
- There should be regular cyber awareness training programmes as the first line of defense against the ever-evolving adversary of cyberattacks.
- Information sharing across government agencies is necessary for building a strong cybersecurity architecture.
- Stakeholders must focus on improving cyber resilience as a key element to tackle the ever-evolving cyber threats facing society.

GLOBAL CYBERSECURITY FORUM HELD IN SAUDI ARABIA, GHANA'S PARTICIPATION

Background

The Global Cybersecurity Forum is an initiative of Saudi Arabia's National Cybersecurity Authority, and it is a platform for the exchange of ideas and further dialogue on the significant challenges and opportunities of cyberspace. The 2022 edition of the Global Cyber Security Forum, organised by the Kingdom of Saudi Arabia, was under the theme: *Rethinking the Global Cyber Order, with other sub-themes on geo-cyber evolution, disruption frontier, cyber economics, future of cyber work and no one left behind*. The themes focused on:

- understanding the evolving international cyberspace order,
- the current and future cybersecurity threats and
- ways to bridge global cyber divides and to ensure that cybersecurity benefits and supports all people and societies.

The event brought together 117 countries, including Ghana, 127 of the world's best minds to advance the global cybersecurity agenda and 9,000 attendees. Among the speakers at the events were the Hon. Minister for Communications and Digitalisation, Mrs. Ursula Owusu-Ekuful and the Director-General of Ghana's Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako.

Ghana was invited to be part of the event due to its modest achievements in cybersecurity development and in connection with the National Cyber Security Awareness Month.

Key Discussion Areas

At a High-level ministerial roundtable discussion, participants examined challenges and proposed solutions on issues relating to:

- Managing the Escalating Cost of Cybersecurity
- Proactively Mitigating the Human Impact of Ransomware (HIR) in Critical National Infrastructure (CNI) Sectors and



- Closing the Talent Gap and Protecting the Most Vulnerable

It was observed from the discussions that cybercrimes are increasing as society gets more digitalised, and that the criminals seem to be a step ahead. As a result, the only option was for countries to invest in capacity in order to increase their efforts to prevent such crimes and to stay resilient.

It was noted that an effective strategy to combat cybercrime and malicious activities in cyberspace was the adoption of a multi-stakeholder approach in which the roles and responsibilities of government agencies and other collaborating partners were clearly defined. Ghana's Joint Cybersecurity Committee (JCC) established by section 13 of the Cybersecurity Act, 2020 (Act 1038) was cited as an example for such collaboration.

Capacity building and awareness creation and the adoption of strategies and frameworks to proactively protect against cybercrime as well as good incidence coordination and response plans were identified as other measures to mitigate the global cost of cybercrimes.

Cyber Diplomacy was further proffered as one of the ways through which state actors can come together to address pertinent issues relating to the protection of Critical National Infrastructure (CNI). Additionally, the ratification of international conventions was noted to help facilitate information sharing in addressing the issue of ransomware, especially, noting that cybersecurity is borderless and some of these crimes can only be solved when countries are able to successfully cooperate with each other.

Regulatory frameworks and legal compliance were further said to be necessary to ensure service providers and professionals meet required standards, and further make it possible for individuals, businesses, and governments to engage the right persons and institutions and to attract the right talents.

There were other related discussions that focused on cooperation as an Imperative to tackle cybercrime, the safety of children in cyberspace and how to Keep children's best interests paramount, among others. These discussions were relevant to Ghana's ongoing cybersecurity development programmes and provided insights for the commencement of the cybersecurity regulatory regime.

Conclusion

Seeking to address topics from geocyber, cybereconomics, cyberconflicts, online child protection and the future of cyber work, the Global Cybersecurity Forum in Saudi Arabia offered diverse perspectives to participating countries. According to experts, the ambition to rethink the global cyber order and plans to include more partnerships and collaboration was in the right direction.

The Ghanaian delegation held bilateral discussions with key personalities in Saudi Arabia's government to collaborate on cybersecurity issues such as capacity building and knowledge sharing. The Government of Ghana was led by the Hon. Minister for Communications and Digitalisation, Mrs. Ursula Owusu-Ekuful, and the Kingdom of Saudi Arabia was represented by H.E. Abdullah bin Amer Alswaha, Minister of Communications and Information Technology.

Key Recommendations

- Collective action is needed to deal with increasing threats from hackers.
- Geopolitics should be used to shape not only cybersecurity, but also the security posture of economies and how countries should design and implement their goals and strategies.
- It is important to create a cohesive diplomatic framework to counter cross-national cybersecurity threats.
- Regulation, innovation, inclusion, cross-sector collaboration, and enforcement have been identified as critical factors to create a safer cyberspace.

WORLD ECONOMIC FORUM'S ANNUAL CYBERSECURITY SUMMIT, GHANA'S PARTICIPATION

Background

The World Economic Forum (WEF) Centre for Cybersecurity hosted its annual cybersecurity summit from November 15-16, 2022, in Geneva, Switzerland, focusing on cyber resilience and the need for leadership and cooperation to deal with the growing threat within the landscape. The Annual Meeting is a focal point for leaders to accelerate the partnerships needed to tackle global challenges and shape a more sustainable and inclusive future.

The summit brought together 100s of the world's foremost cybersecurity leaders and experts from global businesses, governments, international organisations and civil society. The Director-General of Ghana's Cyber Security Authority, Dr. Albert Antwi-Boasiako participated in the event together with selected Chief Executive Officers of Cybersecurity institutions across the world.

Focal areas of discussion

The event participants held discussions that focused on the fact that;

- The success of any organisation's digital transformation depends not only on technology, but also on human capital.
- Malicious actors are increasingly targeting the weakest link in technology systems which is the human beings who interact with them.
- Bridging the gap between cybersecurity



- experts and decision-makers at the highest levels was necessary to reinforce the importance of cybersecurity as a key strategic priority.
- To address global cyber challenges, there was a need for a higher level of collaboration and network with stakeholders whose interests expand beyond national borders.

The discussions tied with Ghana's awareness creation efforts specified under section 60 of the Cybersecurity Act, 2020 (Act 1038) and the five-year National Cybersecurity Awareness Programme dubbed, "A Safer Digital Ghana", which had been launched since October 2018, with a focus on Children, the Public, Businesses and Government.

Further discussions were based on the future of cooperation in a fragmented world; with an emphasis on the current geo-political context. The discussions focused on the implications of the digital landscape and explored opportunities for partnerships and collaborations to strengthen resilience at a global level.

There were discussions that also harnessed opportunities for greater cooperation to improve the state of cybersecurity globally. Participants explored prospects for collaboration with the private sector at a global level in relation to the need for greater regulatory alignment and multistakeholder approaches to policy formulation. The need for a community of "National Cyber Chiefs" to operate in collaboration with the Forum to ensure better engagement with the private sector globally, also featured predominantly.

Conclusion

Ghana's participation in the annual summit was significant as it presented opportunities for collaboration at the highest council level on matters of global importance on cybersecurity matters. The Director-General of the Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako, and the Managing Director of the World Economic Forum (WEF), Mr. Jeremy Jurgens, held bilateral discussions on the sidelines of the Annual Meeting on Cybersecurity, following which it was agreed that the Cyber Security Authority will be collaborating with the WEF on an Initiative titled - 'Public-Private Partnerships on Cybersecurity' in 2023.

Recommendations

- Security awareness is a core element of workplace upskilling and hence people outside the IT and cybersecurity functions need training in the area in order to make better decisions on the design, operation, and oversight of digital infrastructure.
- Public-private sector collaboration is key in addressing cybersecurity challenges.
- Countries should prioritise cybersecurity skills development as part of their cybersecurity development.
- Collaboration at different levels is necessary for cybersecurity development locally and internationally.

ECOWAS COMPUTER SECURITY INCIDENT RESPONSE (CSIRTS) TEAM WEEK



Background

The ECOWAS Commission, as part of the implementation of the West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C) Project, convened the ECOWAS Computer Security Incident Response Teams (CSIRTs) Week from October 24 to 28, 2022 in Bissau, Guinea-Bissau. The event was attended by Cybersecurity representatives from ECOWAS Member States including Mauritania.

The objective of the event was to foster the sharing of knowledge, insight, and best practices amongst Computer Emergency Response Teams (CERTs) within the ECOWAS region and Mauritania. Additionally, the event was aimed at elaborating on the importance of national CERTs on the development of cybersecurity and to facilitate the needed relationships for more efficiency among individual officials and among CERTs.

The event was attended by delegates from Benin, Cabo Verde, Cote d'Ivoire, The Gambia, Guinea-Bissau, Liberia, Nigeria, Senegal, Sierra Leone, Togo, Mauritania and Ghana.

Ghana was represented by two officials from the National CERT of the Cyber Security Authority (CSA). They gave an overview of the establishment of the CERT ecosystem in Ghana and efforts being put in place to establish sectorial CERTs to aid in incident response and coordination across all sectors of the country.

Remarks

Mrs. Rabiyatou Bah
Project Coordinator, OCWAR-C

In her remarks, she expressed her gratitude to the organisers for aiding in the fight against cybercrime and helping to bridge the cybersecurity gap in Africa. She further indicated that the OCWAR-C Project had two main objectives, i.e., to identify the preparedness and operation of the beneficiary countries. She added that the ECOWAS CSIRTs Week was also aimed at Information Sharing and urged all participants to actively participate in the event.

Remarks

Mr. Hamidou Boly
ECOWAS Representative to Guinea Bissau

Mr. Hamidou Boly stated in his remarks that, the ECOWAS Commission is dedicated to helping member countries and Mauritania have a resilient digital ecosystem. He emphasised the economic

importance of a resilient cyberspace and urged all member countries to take advantage of the OCWAR-C Project to build both managerial and technical capacities. He assured participants of continual support from the ECOWAS Commission with regards to the OCWAR-C project and encouraged all participants to make inputs, suggestions and challenges to make the conference a successful one.

Remarks

Representative for Guinea Bissau

In his remarks, he highlighted the various strategies and plans the government of Guinea Bissau is putting in place to streamline cybersecurity practices in the country. He stated that the collaboration with the ECOWAS Commission on the OCWAR-C Project will help fasten such processes. He indicated that a resilient digital economy will improve the country's economy. He urged all participants to be involved in the activities for the week and wished participants the best.

Training

In a two-day training programme, the participants shared ideas on best practices from their respective countries relevant for the development and operationalisation of National CERTs. They were further taken through a Malware Information Sharing Platform (MISP) tool that can be leveraged on by nationals within the ECOWAS region to share information and threat intelligence. According to the instructors, MISP is designed by and for incident analysts, security and Information Communications Technology professionals or malware reversers to support day-to-day operations and to share structured information efficiently. The MISP provides functionalities to support the exchange of information and the consumption of said information by Network Intrusion Detection Systems (NIDS) as well as log analysis tools (SIEMs).

The training on MISP equipped participants to share information among themselves. It served as a model for member countries to practice how to share information among themselves as part of the impending enrolment onto the ECOWAS region MISP. The MISP hands-on training provided the basics for other beneficiary countries without CERT to have an idea of some technical operations of CERT and to appreciate the importance of information sharing.

Conclusion

Mrs. Rabiyatou Bah in her closing remarks thanked all participants for their contributions and commitment to sharing their respective perspectives towards the success of the event. She encouraged all participants to make good use of the training they acquired upon return to their specific countries and as well share knowledge gained with their colleagues.

UNODC WOMEN IN CYBER SUMMIT 2022

Background

The maiden edition of the United Nations Office on Drugs and Crime (UNODC) Women in Cyber (WiC) Summit took off from October 26 - 28, 2022, in Bangkok, Thailand. The event sought to reduce the gender gap across the cybersecurity/cybercrime domain by building a community of inspiring women professionals and offering an opportunity to integrate gender into cybersecurity and cybercrime-related issues. The three-day summit enabled participants to mainstream the gender dimension among cybercrime professionals for the advancement of women in fighting cybercrime and encouraged them to lend a helping hand to other women within the cyber field to allow for greater representation of women in the cyber profession.

The Cyber Security Authority (CSA) was represented by two officials as part of efforts to build capacity and to share knowledge in connection with the National Cyber Security Awareness Month (NCSAM)

Key Discussions

In a keynote speech, the Head of Counter Cybercrime Programming Africa at the UNODC, Ms. Carmen Corbin, urged the female participants to create opportunities to elevate each other at the summit and beyond. She further highlighted the need to encourage men to assist and support women to increase their opportunities.

The CSA participants spoke on two separate panel discussions which focused on "Gender-based Violence Against Women Online and Online Child Sexual Exploitation" and "Women Network in Cyber: The Next Generation". The participants shared experiences on gender-based violence online and child sexual exploitation cases in their respective lines of work. A notable observation was that boys and girls were equally victims of online child sexual exploitation, and it was emphasised that having women in leadership was necessary to help combat the scourge.

Other Panel Discussions highlighted the importance of identifying the right mentor or sponsor to provide relevant career guidance. Further discussions focused on ways in which young girls could be encouraged to take up career paths in cyber and related fields.

Conclusion

The Women In Cyber (WIC) Summit concluded with roundtable discussions on issues women in the field of cyber/IT face on the job. The participants developed localised action plans and were urged to implement these plans when they go back to their country.

Media Engagements

NATIONAL
CYBER SECURITY
AWARENESS MONTH

NCSAM 2022 MEDIA ENGAGEMENTS



As part of efforts to reach the larger Ghanaian population during the National Cyber Security Awareness Month (NCSAM) 2022, a number of media houses gave CSA the opportunity to use their platforms to educate and inform the public.

The public were thus educated and informed about the Cybersecurity Act, 2020 (Act 1038) and what the Authority sought to do by regulating the industry, the importance of NCSAM to the citizenry, and what role the public was expected to play in connection with NCSAM, among others.

Generally, the media was used to intensify awareness creation on Act 1038 and on good cyber hygiene practices, issues related to child online protection and other online sexual offences, among others were discussed.

Some of the shows the Authority participated in are in the table below

S/N	MEDIA CHANNEL	PROGRAMME
1	Joy News Tv	The Law, The Pulse
2	GTV	Talking Point, Breakfast Show
3	UTV	Primetime (10pm) News
4	Asaase Radio	Breakfast Show
5	Kasapa fm / Agoo Tv	Breakfast Show
6	Baina TV - Hausa	Breakfast Show
7	Adoa TV	Breakfast Show
8	Greena Fm (Bono Region)	Breakfast Show
9	Agoo FM (Eastern Region) - Twi	Breakfast Show
10	Eagle FM (Central Region) - Fante	Breakfast Show
11	Hello FM (Ashanti Region) - Twi	Breakfast Show
12	Power Impact Series Show	Online Show
13	Joy Business Social	Online Show

Participation Analysis

Physical and Virtual Participation at events is demonstrated in the table below

S/N	EVENT	DATE	VENUE	NUMBER OF PARTICIPANTS
1	Media Launch of the National Cyber Security Awareness Month (NCSAM) 2022 (Hybrid)	Sep. 14, 2022	Ministry of Information	7,800
2	Launch of Cybersecurity Awareness Programme for the Ghana Armed Forces as part of NCSAM 2022 (Hybrid)	Sep. 30, 2022	Burma Camp	400
3	Official Launch of the National Cyber Security Awareness Month (NCSAM) 2022 (Hybrid)	Oct. 03, 2022	Cedi Conference Centre, University of Ghana	1,890
4	Public Consultation on Framework for the Licensing of Cybersecurity Service Providers, Accreditation of Cybersecurity Establishments and Accreditation of Cybersecurity Professionals and Practices (Physical)	Oct. 05, 2022	NCA Conference Room	103
5	Forum on Ghana Cybersecurity Regulations and Opportunities for Cybersecurity Industry Players and Professionals (Hybrid)	Oct. 06, 2022	College of Physicians and Surgeons, Accra	761
6	Public Consultation on Framework for the Accreditation of Sectoral CERTs (Physical)	Oct. 10, 2022	NCA Conference Room	50
7	Compliance Workshop on Directive for the Protection of Critical Information Infrastructure (Physical)	Oct. 11, 2022	Alisa Hotels, Accra	131
8	National Cybersecurity Challenge for Senior High Schools (Hybrid)	Oct. 17, 2022	GNAT Hall, Accra	1,388
9	Civil Society Forum on Regulating Cybersecurity through Strategic partnership (Physical)	Oct. 19, 2022	Fiesta Royale Hotel, Accra	155
10	Cyber Security Authority /Ghana Association of Bankers Board and Executive Directors briefing on “Ghana's Cybersecurity Act, 2020 (Act 1038); The Bank of Ghana cyber and Information Security Directive; its implications and the Role of Board of directors” (Physical)	Oct. 20, 2022	Marriot Hotel, Accra	160
11	Technical Training on Cybersecurity for selected staff of the Cyber Security Authority and joint Cybersecurity Committee Institutions (Physical)	Oct. 26-28, 2022	Huawei Office, Accra	40

NB: This figure excludes the number of people who were reached through Media engagements and other stakeholder engagements and broadcasts.

Conclusion

The 2022 edition of the National Cyber Security Awareness Month (NCSAM) themed "***Regulating Cybersecurity: A Public-Private Sector Collaborative Approach***" sought to build synergy among public-private sector stakeholders for collaboration and partnership for the implementation of key cybersecurity regulations and to build capacity among critical stakeholders. The month-long event consisted of the official launch, high-level consultative events and awareness creation programmes strategically targeted at key public and private sector institutions, civil society groups, children, and the general public.

The official launch of NCSAM 2022 was marked with key speeches focusing on the importance of collaborations for a successful implementation of the Cybersecurity Act, 2020 (Act 1038). It was announced at these events that from January 2023, all Critical Information Infrastructure Owners, either in the private sector or public institutions, will be required to undergo mandatory compliance checks and audits to ensure the protection of Ghana's critical systems. Additionally, the Ministry of Communications and Digitalisation, working through the Cyber Security Authority (CSA) is committed to the full enforcement of the Cybersecurity Act, 2020 to ensure that from January 2023, no firm will operate a cybersecurity service in the country without a licence granted by the Authority. Ghana's commitment to international cooperation was further demonstrated through the signing of Memoranda of Understanding (MoUs) with Rwanda and Mozambique for collaboration in cybersecurity matters. The highly participated event brought together about 500 participants comprising key stakeholders from government and non-governmental institutions including Ministers of State, Board Members of the CSA, Joint Cybersecurity Committee (JCC) Institutional Heads, Ambassadors and High-Commissioners, CEOs, representatives from industry and academia as well as the media.

Other high-level events which were mainly consultative in nature, touched on the four thematic areas of the Safer Digital Ghana Programme, namely children, the public, businesses, and government. Different stakeholder institutions were also involved as they organised awareness creation sessions for their constituents; this proved to be exceptional, expanding in scope and reach compared to previous events and achieving a greater level of capacity building and awareness creation.

One innovative event worth highlighting was the maiden edition of the National Cybersecurity Challenge where 6 selected Senior High Schools from across the country competed to be the "Cyber Hero".

The CSA is grateful to all stakeholders, sponsors, and partners for their tremendous support in ensuring a successful NCSAM 2022, most importantly, for their contributions to the advancement of the nation's cybersecurity for a secure and resilient digital Ghana.

.

Recommendations

Below are some of the key recommendations made during the NCSAM 2022:

i. Organisations should dedicate a minimum of between 15% to 25% of their ICT budget to cybersecurity for a meaningful and sustainable progress in addressing cybersecurity challenges.

ii. Capacity building and awareness creation programmes should be targeted at all members of an organisation, not only the Information Technology officials.

iii. CSA should come up with manuals that can be used for cybersecurity training and awareness creation purposes.

iv. CSA should interact and engage the public across the country in identifiable local languages on cybersecurity best practices.

v. To help with the efficient management of cybersecurity challenges, CII owners should conduct internal cybersecurity exercises and assessments.

vi. CII owners should cooperate and create confidence with one another in order to strengthen the country's cybersecurity posture.

vii. CII owners in the banking and finance sector were urged to maximise their efforts in complying with the CII registration processes.

viii. Information sharing amongst financial institutions must be improved to effectively tackle cybersecurity related issues.

ix. Business leaders should consider career guidance and professional development programs towards developing their cybersecurity posture.

x. Financial institutions should intensify awareness creation on cyber risks and promote appropriate incident reporting and response practices.

xi. There was a call for an agile cybersecurity regulation and the need to be up to date with cybersecurity needs and development.

Steering Committee for NCSAM 2022

i. Hon. Mrs. Ama Pomaa Boateng (Co-Chair) - Deputy Minister for Communications and Digitalisation

ii. Dr. Albert Antwi-Boasiako (Co-Chair) - Ag. Director-General of the Cyber Security Authority (CSA)

iii. Ms Adjoa Asamoah - Bank of Ghana

iv. Mr. Derek Laryea - Private sector

v. Mr. Palgrave Boakye-Danquah – Ministry of Information

vi. Ms Angela Adu Ampofo - MTN

vii. Mr. Benjamin Ofori - Cyber Security Authority (CSA)

viii. Mr. Alex Oppong - Cyber Security Authority (CSA)

ix. Mrs Mercy Araba Kertson - Cyber Security Authority (CSA)

x. Ms. Jennifer Mensah - Cyber Security Authority (CSA)

xi. Ms Faustina Maner Angmor - Cyber Security Authority (CSA)

xii. Capacity Building and Awareness Creation Team - Cyber Security Authority (CSA)



Editorial Team

Rapporteurs

i. Andrew Owusu-Agyemang, Legal and Compliance

ii. Sharon Paulina Boye - Communications

iii. Jael Amponsah-Bempah – Child Online Protection

iv. Andrew Asamoah-Kissiedu, Critical Information Infrastructure Protection

v. Naa Aku Shika Anum, DG's Secretariat

vi. Joseph Antwi Attoh, Computer Emergency Response Team

vii. Abigail Kaki Onyame, Child Online Protection

viii. Sherifa Awinbun Atangiba, Technology Standards

Editors

i. Faustina Maner Angmor, Communications

ii. Ingrid Serwah Asare, Legal and Compliance

iii. Kwamina Amponsah Dadzie, Communications

iv. Patricia Adafienu, Capacity Building and Awareness Creation

v. Cynthia Maku Dassinor, Communications

vi. Emmanuella Darkwah, International Cooperation

Graphic Design & Photography

i. Erik Gordon-Quaicoe, Communications

Photo Gallery

NATIONAL
CYBER SECURITY
AWARENESS MONTH

Media Launch Event










Cyber Security Authority


Cyber Security Authority


MINISTRY





NCSAM Official Launch



























CYBER SECURITY
AWARENESS MONTH
2022
CYBERSECURITY
A Public - Private Sector
Collaborative Approach













Public Consultation on Framework for the Licensing of Cybersecurity Service Providers












CYBER SECURITY
AUTHORITY
(CSA)

Forum on Ghana's Cybersecurity Regulations for Industry Players and Professionals



Public Consultation for the Development of an Accreditation Framework for the Accreditation of Sectoral CERTs



Compliance workshop on the directive for the protection of Critical Information Infrastructure for CII Owners













Training Course on Cybercrime for Judges and Prosecutors











Civil Society Forum




Public Financial Management
HON. AMA POMAA BOATENG
CYBER SECURITY AUTHORITY



















Ghana Association of Banks Event















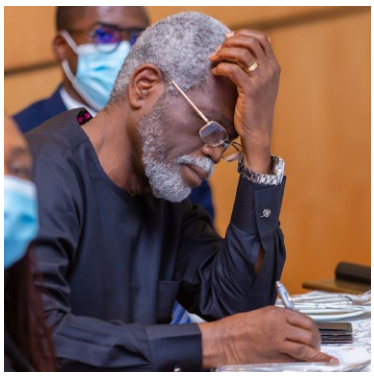
BOARDS AND EXECUTIVE DIRECTORS BRIEFING ON
S CYBERSECURITY ACT, 2020;
AND INFORMATION SECUR
ROLE OF BOARD OF
REGU
CYBERS
A Public
Collabor
ZENITH
Stanbic Bank
















GAB
GHANA

CSA engages members of the Telecommunications Chamber











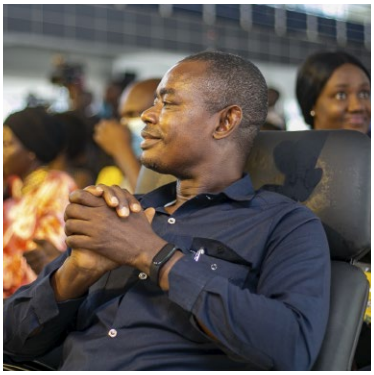








National Cybersecurity Challenge 2022













GAB





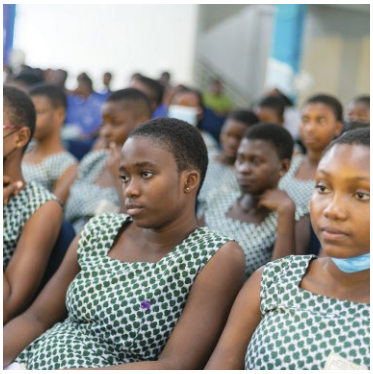

NATIONAL
CYBERSECURITY
CHALLENGE
who will be the
Cyber Hero?




GDS
AFRICA
AEOS
ITCONSORTIUM
MAXAM
Stanbic Bank
unicef
HUAWEI
innovare




NATIONAL
CYBERSECURITY
CHALLENGE










Partners


FREEDOM
AND
JUSTICE


NATIONAL COMMUNICATIONS
NCA
AUTHORITY


WORLD BANK GROUP


HUAWEI


ITU


COUNCIL OF EUROPE
CONSEIL DE L'EUROPE


german
cooperation
DEUTSCHE ZUSAMMENARBEIT


BANK OF GHANA
EST.1957


unicef

Sponsors



Media Partners





CYBER SECURITY AUTHORITY (CSA)

A SECURE AND RESILIENT DIGITAL GHANA



www.csa.gov.gh

Cyber Security Authority Ghana