



MINISTRY OF
COMMUNICATIONS



NATIONAL
CYBER SECURITY
CENTRE

Securing Ghana's Digital Journey...



NATIONAL
CYBER SECURITY
AWARENESS MONTH

2020 Report

CYBERSECURITY
IN THE ERA OF
COVID-19

Contents

i	ACKNOWLEDGEMENT	ii	ACRONYMS
iii	EXECUTIVE SUMMARY	v	GHANA'S CYBERSECURITY GOVERNANCE - LEADERSHIP
vi	NATIONAL CYBER SECURITY INTER-MINISTERIAL ADVISORY COUNCIL (NCSIAC)	vii	NATIONAL CYBER SECURITY TECHNICAL WORKING GROUP (NCSTWG)
viii	KEYNOTE STATEMENT	ix	KEYNOTE STATEMENT Ghana's Cybersecurity Initiatives
xi	KEY STATEMENT Ghana's Incident Reporting Initiative		
01	FORMAL OPENING OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2020	02	BACKGROUND
03	SESSION A - Remarks & Addresses LAUNCH OF NATIONAL CYBER SECURITY AWARENESS MONTH 2020		
05	WELCOME ADDRESS Mr. Eric Kofi Ofosu Nkansah, Acting Managing Director, Accra Digital Centre	06	OPENING REMARKS Dr. Albert Antwi-Boasiako, National Cybersecurity Advisor
08	REMARKS Madam Anne-Claire Dufay, Country Representative, UNICEF Ghana	09	REMARKS Mr. Christopher Lamora, Deputy Chief of Mission/Chargé D'Affaires, U.S. Embassy Ghana
10	REMARKS Hon. Cynthia Mamle Morrison, Minister for Gender, Children and Social Protection	11	REMARK & SIGNING OF COP REPORTING CONTRACT: Internet Watch Foundation (IWF)
13	KEYNOTE ADDRESS, OFFICIAL LAUNCH OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2020 AND LAUNCH OF THE CHILD ONLINE PROTECTION REPORTING PORTAL Hon. Alexander K.K. Abban, Deputy Minister for Communications		
WEEK 1			
CHILD ONLINE PROTECTION		16	
17	CHILD ONLINE PROTECTION WORKSHOP FOR TELECOMMUNICATIONS SERVICE PROVIDERS	25	CHILD ONLINE PROTECTION CYBER HYGIENE BEST PRACTICES FOR SCHOOL CHILDREN
31	CHILD ONLINE PROTECTION CYBER HYGIENE BEST PRACTICES FOR PARENTS AND GUARDIANS	37	LAUNCH OF DATA PROTECTION SOFTWARE AT THE PREMISES OF THE DATA PROTECTION COMMISSION

WEEK 2

BUSINESS FOCAL AREA

41

42

WORKSHOP ON IMPACT OF COVID-19
ON GHANA'S DIGITALISATION AGENDA

46

CYBERSECURITY WORKSHOP ON
MOBILE MONEY FRAUD

51

WORKSHOP ON CYBERCRIME
SCHEMES IN THE ERA OF COVID-19

56

WORKSHOP ON MAINTAINING
PRIVACY ONLINE IN THE ERA OF
COVID-19

60

JOINT FREEDOM ONLINE COALITION (FOC)/ NATIONAL CYBER SECURITY CENTRE
(NCSC) CONFERENCE ON DIGITAL INCLUSION IN THE ERA OF COVID-19

WEEK 3

PUBLIC FOCAL AREA

63

64

CYBERSECURITY FORUM WITH
INDUSTRY PLAYERS

74

ROUNDTABLE DISCUSSION
Embracing Change and Digital
Transformation in the Era COVID-19

79

WORKSHOP ON ADDRESSING
CYBER-FRAUD IN GHANA'S
FINANCIAL SECTOR

83

WORKSHOP ON CRITICAL INFORMATION
INFRASTRUCTURE (CII) PROTECTION AND
RESILIENCE - PART 1

85

NATIONAL CYBER RISK ASSESSMENT
(NCRA) WORKSHOP - Part 1

88

WORKSHOP FOR SECTORAL COMPUTER EMERGENCY
RESPONSE TEAMS (CERTS) ON LESSONS LEARNED IN
THE ERA OF COVID-19 - VIRTUAL PLATFORM

91

WORKSHOP ON CYBERCRIME &
ELECTRONIC EVIDENCE HANDLING
FOR CRIMINAL JUSTICE SECTOR

94

LAUNCH OF THE NATIONAL INFORMATION
TECHNOLOGY AGENCY SECURITY
OPERATIONS CENTRE (NITA SOC)

WEEK 4

GOVERNMENT FOCAL AREA

100

101

WORKSHOP ON CRITICAL INFORMATION
INFRASTRUCTURE PROTECTION AND
RESILIENCE - Part 2

104

NATIONAL CYBER RISK ASSESSMENT
(NCRA) WORKSHOP - PART 2

107

WORKSHOP ON LESSONS LEARNED
BY THE TELECOMMUNICATIONS
SECTOR DURING COVID-19 CRISIS

111

WORKSHOP ON CYBERCRIME &
ELECTRONIC EVIDENCE HANDLING
FOR CRIMINAL JUSTICE SECTOR

115

REGIONAL CAPACITY BUILDING AND
SENSITISATION EXERCISE

124

CONCLUSIONS &
RECOMMENDATIONS

126

PHOTO
GALLERY

131

PLANNING
PHASE

132

PARTNERS
& SPONSORS

Acknowledgement

The progress and accolades of Ghana's Cybersecurity development witnessed at the local and international level is largely as a result of the Government's political commitment demonstrated by His Excellency Nana Addo Dankwa Akufo-Addo's prioritisation of Ghana's digitalisation agenda coupled with strategic investments in cybersecurity. The Minister for Communications expresses her sincerest gratitude to the president's vision, dedication, and leadership exhibited towards securing Ghana's digital ecosystem. The Ministry also wishes to thank His Excellency, the Vice President, Dr. Alhaji Mahamudu Bawumia for his commitment to prioritising the digitalisation agenda in Ghana, complimented by proactive cybersecurity initiatives for a ttsecured cyberspace. Appreciation goes to the various roles played by Members of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) in providing policy direction for the country's cybersecurity development. Members of the National Cyber Security Technical Working Group (NCSTWG) are duly acknowledged for their efforts and hard work in providing technical advice on the country's cybersecurity agenda. An expression of gratitude is also extended to the Event Planning Committee and the various sub-committees for the excellent work in organising the National Cyber Security Awareness Month (NCSAM) 2020.

The Ministry of Communications is highly grateful to our sponsors and international partners for their support and commitment through various investments in the Ministry of Communications' cybersecurity efforts and initiatives. The Ministry highly commends individuals, civil society, businesses, academia, government and non-government organisations for their participation in the month-long event which has significantly contributed to capacity building and awareness creation on cybercrime trends and improving cybersecurity awareness among children, the public, businesses, and government for a Safer Digital Ghana.

Mrs. Ursula Owusu-Ekuful (MP)
Minister for Communications

Acronyms

AU	African Union	GSM	Global System for Mobile Communication
ADC	Accra Digital Centre	ICT	Information and Communications Technology
AFCFTA	African Continental Free Trade Area	IOTS	Internet of Things
BNC	Bureau of National Communications	ISACA	Information Systems Audit and Control Association
BNI	Bureau of National Investigations	IT	Information Technology
BOG	Bank of Ghana	IWF	Internet Watch Foundation
CERT	Computer Emergency Response Team	MOC	Ministry of Communications
CERT-GH	National Computer Emergency Response Team	MFWA	Media Foundation for West Africa
CID	Criminal Investigations Department	NCA	National Communications Authority
CI	Critical Infrastructure	NCCE	National Commission for Civic Education
CMM	Capacity Maturity Model	NCSAM	National Cyber Security Awareness Month
CII	Critical Information Infrastructure	NCSC	National Cyber Security Centre
COP	Child Online Protection	NCSIAC	National Cyber Security Inter - Ministerial Advisory Council
C-PROC	Cybercrime Programme Office	NCSIF	National Cyber Security Institutional Framework
CST	Communications Service Tax	NCPS	National Cybersecurity Policy & Strategy
DOS	Denial of Service	NCSTWG	National Cyber Security Technical Working Group
DDOS	Distributed Denial of Service	NITA	National Information Technology Agency
DPC	Data Protection Commission	OCWAR-C	Organised Crime West Africa Response on Cybersecurity and Fight Against Cybercrime
ECA	Electronic Communications Act	POC	Points of Contact
ECOWAS	Economic Community of West Africa States	SOC	Security Operations Centre
EOCO	Economic and Organised Crime Office	UNICEF	United Nation International Children's Emergency Fund
ETA	Electronic Transactions Act	USD	United States Dollar
EU	European Union	WEF	World Economic Forum
FIC	Financial Intelligence Centre	WTO	World Trade Organisation
GCNET	Ghana Community Network Services		
GCSCC	Global Cyber Security Capacity Centre		
GJA	Ghana Journalists' Association		
GIFEC	Ghana Investment Fund for Electronic Communications		
GLACY+	Global Action on Cybercrime Extended		
GSMA	Global System for Mobile Communication Association		

Executive Summary

The National Cyber Security Centre (NCSC) of the Ministry of Communications, in implementing the five-year National Cybersecurity Awareness Programme dubbed A Safer Digital Ghana, launched by H.E. Alhaji Dr. Mahamadu Bawumia on October 1, 2018, is stepping up national efforts to raise awareness on cybercrimes and improve Ghana's cybersecurity readiness in all sectors of the Ghana cyber ecosystem. Key among the initiatives under the Safer Digital Ghana Campaign is the organisation of the annual National Cyber Security Awareness Month (NCSAM) in October which began in 2018.

The National Cyber Security Awareness Month aims to enhance the country's cybersecurity culture and attitude. The NCSAM 2020, built on the work of previous editions is a fundamental component of national effort to build capacity and raise awareness on cybercrimes and the need to improve on Ghana's cybersecurity readiness among children, the public, businesses and government.

Under the theme - Cybersecurity in the era of COVID-19, NCSAM 2020 showcased the preparedness of government, private sector and other stakeholders towards cybersecurity and the prevention of cybercrime with increased reliance on digital technology as a result of the rapid transformation driven by Information and Communications Technology (ICT) and high dependence on technology for socio-economic development. The COVID-19 pandemic has further heightened the increased relevance of ICT especially for the socio-economic development of states. Governments, businesses and individuals' activities are mainly facilitated and coordinated on digital platforms. This has caused a corresponding surge in the number of cybersecurity incidents such as ransomware, banking fraud, data leakage and disruptions in service delivery of Critical Information Infrastructures (CIIs). This has further increased due to the need for

physical and social distancing as a result of the pandemic.

As connectivity is scaled up as part of the government's digitalisation agenda, risks in exposure to cybercrime and cyber-attacks increase and susceptibility to attacks by cybercriminals become high. Successful attacks against any of these critical Information and ICT Infrastructure aimed at fulfilling the goals of the digitalisation agenda can disrupt socio-economic activities in a very significant manner.

Cybersecurity in this era has therefore become imperative to all stakeholders – Children, the Public, Businesses and the Government. Key strategic and priority initiatives implemented over the past three and half years such as the establishment of National and Sectoral Computer Emergency Response Teams (CERTs) and Security Operations Centres (SOCs), the launch of the Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) and the ratification of both the Convention on Cybercrime (Budapest Convention) and African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) have improved incident response as well as the state of cybersecurity readiness. Additionally, due to the fact that the wider population has resorted to digital platforms for activities, the National Cyber Security Centre (NCSC), through the Ministry of Communications (MoC), leveraged the dependency on digital services to intensify the capacity building and awareness creation efforts on cybercrime/cybersecurity. COVID-19 is a crisis that has changed our way of life and the NCSAM 2020 provided the opportunity to educate the public on cyber risks as well as countermeasures. It also highlighted the Government's achievements in the area of cybersecurity within the past three and half years. It provided an opportunity for the promotion of the Cybersecurity/Cybercrime Incident Reporting Points of Contact (PoC) through regional media outlets and stakeholder

**THIS YEAR'S EVENT
CONSTITUTED A
MONTH-LONG PLANNED
CAPACITY BUILDING
AND AWARENESS
CREATION PROGRAMME
FILLED WITH ACTIVITIES
DELIVERED ACROSS ALL
THE SIXTEEN REGIONS
OF THE COUNTRY**

groups to facilitate reporting of cybercrime/cybersecurity incidents and consequently improve local and international cooperation and partnerships to fight cybercrime and improve on cybersecurity. Stakeholders in public and private spaces established and strengthened business and professional networks through the various events.

This year's event constituted a month-long planned capacity building and awareness creation programme filled with activities delivered across all the sixteen regions of the country. Kick-starting activities for the month-long event, the Ministry of Communications through the NCSC officially launched the NCSAM 2020 and the Child Online Protection Internet Watch Foundation (IWF) Portal on October 1, 2020, at the Accra Digital Centre. The Child Online Protection Internet Watch Foundation reporting portal is to facilitate the identification, assessing, reporting, blocking, and removal of Child Abuse Materials (CAM) from the internet, to promote safer use of internet-based services for children. With the support of UNICEF Ghana, the NCSC developed a Child Online Protection (COP) Internet Watch Foundation (IWF) reporting portal in response to online risks associated with children such as cyberbullying, online grooming, circulation of inappropriate content in the use of the internet, especially during this pandemic. The launch and operationalisation of the reporting portal will safeguard children and young people from risks associated with their digital experiences. Additionally, regional cybercrime/cybersecurity sensitisation exercises targeted at selected professional bodies, and media houses across the sixteen (16) regions nationwide were organised from October 2-23, 2020 to educate students who were home at the time, key professionals such as journalists, security service personnel and the general public, on the need to observe proper cyber hygiene protocols. There was also a cybercrime and electronic evidence handling workshop for the law enforcement sector in both the northern

and southern sectors of Ghana, which followed the launch of the NCSAM 2020. Over thirty media houses and professional bodies were also visited across Ghana.

Due to the COVID-19 pandemic, the NCSC deviated from the norm of a grand climax week that has become associated with NCSAM. Instead, concurrent high-level events were held throughout the month. A hybrid format which comprised physical engagements (under strict COVID-19 protocols) and the utilisation of available virtual platforms and media channels geared towards strengthening media collaboration efforts was adopted. These included thought-leadership sessions, workshops, lectures, demonstrations, training sessions, and media engagements. The formal launch and high-level events took place at the Accra Digital Centre (ADC) with limited attendance while leveraging on virtual platforms and media outlets to broadcast proceedings.

Paramount among the events were the:

- ➔ Launch of National Child Online Protection(COP) Internet Watch Foundation (IWF) Reporting Portal
- ➔ Cybersecurity Roundtable Forum – Impact of COVID-19 on Ghana's Digitalisation Agenda & Cybersecurity Considerations
- ➔ Cybersecurity Forum with Industry Players
- ➔ Launch of the Security Operations Centre (SOC) at the National Information Technology Agency (NITA).

The month's awareness programme witnessed the participation of high-profile personalities including Ministers of State, dignitaries and stakeholders from government and non-government institutions, civil society groups, academia, private sector, professional/industry associations, interest groups, the media and representation from Ghana's cybersecurity international partners and diplomatic corps.

GHANA'S CYBERSECURITY GOVERNANCE - Leadership



President of the Republic of Ghana

H.E. NANA ADDO DANKWA
AKUFO-ADDO



Vice President of the Republic of Ghana

DR. MAHAMUDU
BAWUMIA



Minister for Communications

HON. URSULA
OWUSU-EKUFUL



Deputy Minister

HON. GEORGE NYENYI
ANDAH



Deputy Minister

HON. ALEXANDER K.K.
ABBAN

NATIONAL CYBER SECURITY INTER-MINISTERIAL ADVISORY COUNCIL (NCSIAC)

Minister for Communications

HON. URSULA
OWUSU-EKUFUL



Minister for Justice & Attorney General

HON. GLORIA AFUA AKUFFO



Minister for Finance & Economic Planning

HON. KEN OFORI-ATTA



Minister for the Interior

HON. AMBROSE DERY



Minister for Foreign Affairs
& Regional Integration

HON. SHIRLEY AYORKOR
BOTCHWAY



Minister for Defence

HON. DOMINIC NITIWUL



Minister for National Security

HON. ALBERT KAN-DAPAAH

NATIONAL CYBER SECURITY TECHNICAL WORKING GROUP (NCSTWG)

National Cybersecurity Advisor

**DR. ALBERT
ANTWI-BOASIAKO**



Joe Anokye

National Communications Authority
(NCA)



Richard Okyere Fosu

National Information Technology
Agency (NITA)



Patricia Adusei-Poku

Data Protection Commission (DPC)



Yvonne Atakora Obuobisa

Office of the Attorney-General & Ministry
of Justice



Justice Afia Serwah Asare-Botwe
Judicial Service



Lt. Col. Elikem Fiamavle
Ghana Armed Forces (GAF)



ACP Dr. Herbert Gustav Yankson
Criminal Investigations Department
(CID)



Kwabena Adu-Boahene
Bureau of National Communications
(BNC)



Kofi Boakye
Financial Intelligence Centre (FIC)



John Fummey
Bank of Ghana (BoG)



Nana Osei Tutu
National Security Council Secretariat



Jacob Pupilampu
Economic and Organised Crime Office
(EOCO)



Eric Akumiah
Ministry of Communications (MoC)



Matilda Wilson
National Identification Authority
(NIA)



Gen. Nicholas Andoh
Defence Intelligence



Tim Coleman
Bureau of National Investigations
(BNI)



Ken Baiden
Bureau of National Investigations
(BNI)



Alexander Yeboah
Research Department



Madam Adisa Yakubu
Ministry of Foreign Affairs &
Regional Integration



Nana Kofi Asafu-Aidoo
Ghana Domain Name Registry



Keynote Statement

H.E. Nana Addo Dankwa Akufo-Addo

President of the Republic of Ghana

Ghana is highly aware of the relevance and key role Information Technology is playing in our world today. The digital sphere is progressively advancing to improve lives, and it is our goal to not be left behind. That is why we have taken initiatives to digitalise our government systems and continue to engage with private sectors and the public to secure our digital agenda. These developments have created an ease for people and businesses to operate.

The unanticipated COVID-19 pandemic made Information Technology an ever-growing necessity. The world witnessed a shift from free movement to online and virtual working to sustain the continuity of economies. What this meant was that businesses and transactions have become even more digital and this led to a rise in cyber threats and

attacks. This circumstance has also pushed Government to address the issue of digital gap and having a more connected Ghana. These opportunities have presented cybercriminals with access to a wider array of sensitive information and data.

This issue led to intensifying the cybersecurity efforts in the country. Major sector targets included financial and communications sectors. Much attention has been paid to electronic money users, financial service providers, telecommunication service providers, with measures having to be put in place to secure the safety and privacy of individuals and organisations.

The National Cyber Security Centre through its Computer Emergency Response Team (CERT-GH) and incident reporting has been working

with the relevant sector bodies to combat some of these crimes. There is currently a Cybersecurity Act before parliament awaiting approval. This Act will extend the mandate of the Centre in its role as the watchdog of Ghana's cyber ecosystem. The existing and prospective policies on the area of cyber security and management are to guide in promoting efficiency and security. Ghana is hopeful to do more in creating a secure and safe ecosystem.

The above development is an indication of how Ghana is catching up with the global digital experience.

Keynote Statement

A portrait of Hon. Ursula Owusu-Ekuful, a Black woman with short dark hair in a natural style, wearing round glasses and large hoop earrings. She is smiling and wearing a colorful patterned top. The background is a solid red color.

Hon. Ursula
Owusu-Ekuful

Minister for Communications

GHANA'S CYBERSECURITY INITIATIVES

Minister for Communications

HON. URSULA OWUSU-EKUFUL

The theme for this year's National Cyber Security Awareness Month (NCSAM), Cybersecurity in the Era of COVID-19 presents us with an opportunity to explore vulnerabilities and opportunities in the digital space. Dependence on digital technologies has deepened due to the pandemic. We have witnessed technology evolve at a faster pace to meet increasing demands, which has benefitted individuals who now find themselves functioning remotely.

Nonetheless, the negative cybersecurity impacts of the online shifts have tagged 2020 as a year of growing cyber pandemic. Cyber criminals around the world undoubtedly have capitalised on this crisis. Phishing attacks, malspams and ransomware attacks are some of the means attackers are using to bait people due to majority of people now having to work and interact remotely due to COVID-19.

In this new environment, the Ministry of Communications through the National Cyber Security Centre is working steadily and the NCSC is hopeful for approval of its Cybersecurity Act, which will promote its regulatory functions as Government continues to work to increase accessibility and use of digital technologies.

In addition to the Bank of Ghana Security Operations Centre (BoG - SOC), we are set to launch another SOC at the National Information Technology Agency (NITA), to boost monitoring, reporting and incident management of cyber threats and attacks. In these uncertain times, having such interventions are necessary and critical for the effective operationalisation of cybersecurity.

We will not rest on our shoulders in this time, but rather, I urge all stakeholders to take on their responsibilities in order for us to have a resilient cybersecurity.



Keynote Statement

Dr. Albert
Antwi-Boasiako

National Cybersecurity Advisor

GHANA'S INCIDENT REPORTING INITIATIVE

Ghana has shown tangible deliverables concerning cybersecurity development globally and in the sub-region because of the President of the Republic's commitment towards improving cybersecurity efforts to build a digital economy coupled with efforts and support of the Ministry of Communications. The political commitment towards cybersecurity has set Ghana apart on the continent, this represents the government's vision for the digital future of the country. Initiatives such as the Cybercrime/Cybersecurity Incident Reporting Points of Contact (POC) and the continuous efforts in awareness creation enable Ghana to share its experience and expertise with other countries, within the continent.

The National Cyber Security Centre is committed to contributing to building a stronger cybersecurity ecosystem within Africa based on shared experiences and a collective approach to securing the cyber ecosystem. The collaborative efforts approach has a body such as the National Cyber Security Technical Working Group (NCSTWG) constituted by agencies whose mandate border on Cybercrime/Cybersecurity-related issues and work collectively with the NCSC towards enhancing the state of security in cyberspace.

Furthermore, Ghana has been privileged to have friends from the International Community who share in the vision of the government in creating a resilient digital ecosystem. The United Nations, Council of Europe, the European Union, the World Economic Forum, UNICEF, the African Union, ECOWAS Commission and the Security Governance Initiative of the US Government have continuously supported the work of the Centre.

The launch of the Cybercrime/Cybersecurity Incident Reporting Points of Contact (POC) is a milestone that symbolises collective work done to ensure that the national mandate in addressing cybercrime in the country is achieved.

Due to the massive reliance on ICT devices for day to day transactions and interactions, a successful infiltration of these systems and platforms will not only undermine confidence in the digitalisation efforts of the country but will have a detrimental impact on the economic activities of individuals. Hence, citizens need to have reliable channels through which they can immediately and effectively report such attacks when they occur before it has ruinous effects. The POC demonstrates the country's cybersecurity readiness and ability to establish the true state of cybercrime and the state of its cybersecurity. This initiative cannot be operationalised without the involvement of the private sector, the media and the public.

FORMAL OPENING OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2020 & LAUNCH OF THE CHILD ONLINE PROTECTION REPORTING PORTAL



CYBERSECURITY
IN THE ERA OF
COVID-19



NATIONAL
CYBER SECURITY
AWARENESS MONTH

Background

The Ministry of Communications (MoC), through the National Cyber Security Centre (NCSC), has a commitment to achieve the objectives set out in Ghana's National Cybersecurity Awareness Programme, dubbed A Safer Digital Ghana campaign, which was launched by the Vice President, His Excellency Alhaji Dr. Mahamudu Bawumia on October 1, 2018, during the National Cyber Security Awareness Month (NCSAM). The campaign, which focuses on four thematic areas (Children, the Public, Businesses, Government), aims to tackle the menace of cybercrime and improve Ghana's cybersecurity readiness through capacity building and awareness creation.

The 2020 edition of the NCSAM, organised under the theme 'Cybersecurity in the Era of COVID-19' was launched on October 1, 2020, at the Accra Digital Centre. The event witnessed a gathering of key personalities, in the cybersecurity ecosystem. As part of the event, the Child Online Protection Reporting Portal developed by the NCSC with support from UNICEF Ghana was launched. The Child Online Protection Reporting Portal is a joint partnership of the NCSC with the support of UNICEF Ghana and the Internet Watch Foundation to ensure proper monitoring and sanitisation of content put on the internet. The Internet Watch Foundation (IWF) is a registered charity based in Cambridgeshire, England and its remit is "to minimise the availability of online sexual abuse content, specifically child sexual abuse images and videos hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK." The IWF also helps in the identification, assessment, reporting and removal of illegal child online abuse imagery to promote safer use of internet-based services

for children. The NCSC, before the launch of the COP reporting portal, engaged with key stakeholders concerned with the welfare of children to deliberate on the intricacies associated with the proposed partnership with IWF. An agreement was reached by stakeholders that, the COP reporting portal is a good initiative and will assist Ghana in terms of international cooperation, particularly for the blocking, take-down and removal of Child Abuse Materials (CAM). The objective of the COP reporting portal is to create an online community that is safe and beneficial to everyone, especially children. It will further align with and augment the work of the Cybercrime / Cybersecurity Incident Reporting Points of Contact (PoC) in the identification, reporting and removal of illegal Child Abuse Materials (CAM) from internet-based services for children and as well inform the public on hotline and SMS codes for receiving calls and messages.

OVER THIRTY-NINE
THOUSAND (39,000)
CITIZENS WERE
REACHED OUT TO
THROUGH RADIO
AND TELEVISION
ENGAGEMENTS IN
EACH REGION



LAUNCH OF NATIONAL CYBER SECURITY AWARENESS MONTH 2020

As a priority and strategic measure to improve on the cyberculture among Ghanaians, which was declared low, per the findings from the cybersecurity capacity maturity assessment conducted by the Global Cyber Security Capacity Centre (GCSCC) in 2018, the Ministry of Communications (MoC) through the National Cyber Security Centre (NCSC) has been implementing a number of specific initiatives outlined in the National Cybersecurity Awareness Programme dubbed A Safer Digital Ghana launched by H.E Alhaji Dr. Mahamudu Bawumia on October 1,

2018. The programme is targeted at four thematic areas i.e. Children, the Public, Business and Government.

Paramount among the initiatives of 'A Safer Digital Ghana' programme being implemented include the National Cyber Security Awareness Month (NCSAM), an annual event scheduled for October to intensify capacity building and awareness creation efforts on cybercrimes and improve on Ghana's cybersecurity readiness. The NCSAM which commenced as a week-long event in 2017 has transformed into a month-long event and has witnessed successful organisation and observation for the past three years. A number of key milestone initiatives to improve the cybersecurity landscape and readiness have been birthed out of the previous editions of the NCSAM. This includes the deployment of the Cybercrime/Cybersecurity Incident Reporting

Points of Contact (POC), the launch of the National Communications Authority Computer Emergency Response Team (NCA-CERT) and the Bank of Ghana Security Operations Centre (BoG-SOC) to manage cybersecurity incidents at the telecommunications and financial sectors respectively, among others.

The 2020 edition of the NCSAM dubbed Cybersecurity in the Era of COVID-19 was earmarked to highlight the relevance of cybersecurity for socio-economic activities, particularly in the era of the COVID-19 pandemic. In addition, the event presented an opportunity to demonstrate the state of cybersecurity preparedness especially as there is an increased dependence on ICTs for socio-economic sustenance. Among the key strategic and priority

investments and initiatives implemented over the past three and half years in the cybersecurity ecosystem include the revision of the National Cybersecurity Policy & Strategy (NCPS) to reflect current cybersecurity development trends; development of a draft Cybersecurity Bill to regulate the cybersecurity ecosystem; Revision of the National Child Online Protection (COP) Framework to guide policy development and implementation of COP initiatives and the implementation of a five (5)-year National Cybersecurity Awareness Programme, dubbed 'A Safer Digital Ghana' to create cybercrime and cybersecurity awareness among Children, the Public, Businesses and Government. The launch of the NCSAM 2020 on Thursday, October 1, 2020 at the Accra Digital Centre, Ring Road West-Accra witnessed the gathering of high-profile personalities from ministries, government and non-governmental organisations, civil society organisations, industry players, businesses, the media, local and international partners, and Ghana's diplomatic corps. The event, like the rest of the awareness month activities,

was conducted in a hybrid format comprising physical engagement under strict COVID-19 protocols and the use of virtual and traditional media platforms. As part of the launch of the NCSAM 2020, a Child Online Protection (COP) reporting portal – a milestone initiative was launched, in collaboration with the Internet Watch Foundation (IWF), to climax the day's activity. The COP reporting portal which is to augment the existing Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) will significantly contribute to cybersecurity incident reporting mechanisms. It is child user-friendly and is meant to enhance the reporting procedures pertaining to Child Sexual Abuse Material (CSAM) available on the internet. This will ensure the blocking, filtering and takedown of illicit content relating to children and young people's activities online when a report is made to that effect. The portal will holistically improve the work of the NCSC in the implementation of stronger actions geared towards addressing child online abuses.



Eric Kofi OFOSU NKANSAH

Ag. Managing Director, Accra Digital Centre

Welcome Address

Mr. Eric Ofosu Nkansah in his welcome address expressed delight that the Accra Digital Centre (ADC) was considered to host the 2020 edition of the NCSAM. He presented a brief background about the ADC and its mandate in the support and promotion of digital innovation and entrepreneurship which reflects the basis for cybersecurity development in the country. Accelerating ICT business growth and development, business development training programmes to startups and other companies, assistance with transforming ideas into businesses, job creation, support for digital skills and innovation programmes, among others as part of the core objectives of the ADC, he elaborated. Given this, cybersecurity efforts, therefore, become imperative to support the digital initiatives government is pursuing which have contributed to the

ADC's commitment to host the NCSAM event. In concluding, he outlined the programme of activities scheduled for the month-long event and recommended a fruitful deliberation to build a trustworthy digital ecosystem to secure Ghana's digital dividends.



Dr. Albert ANTWI-BOASIAKO

National Cybersecurity Advisor



Opening Remarks

Dr. Albert Antwi-Boasiako remarked that cybersecurity has become a prominent issue especially in the era of COVID-19 which informed the convergence of the relevant stakeholders for the NCSAM event. Outlining some key milestones that the National Cyber Security Centre (NCSC) has achieved over the past three and half years of existence, he reiterated the commitment of the Government through the National Cyber Security Centre under the Ministry of Communications to secure the country's digital ecosystem.

The Advisor gave a brief background about the NCSC and the priority and strategic investments and

initiatives being implemented within the country's cybersecurity ecosystem noting that “the Centre which began as a secretariat in 2017 was focused on developing the National Cyber Security Institutional Framework (NCSIF) of the country's cybersecurity architecture which has been a success with key political commitment from the President who is spearheading our cybersecurity course, the Vice President with his digital innovation agenda and the Minister for Communications for her commitment to ensuring the realisation of our cybersecurity development”.

To buttress his assertion that the country is on the right path of cybersecurity development, Dr. Antwi-Boasiako outlined a number of priority and strategic investments and initiatives implemented in Ghana's cybersecurity ecosystem

which includes, the revision of the National Cybersecurity Policy and Strategy (NCPS) to reflect current cybersecurity developments and trends consistent with best practices; a draft Cybersecurity Bill pending Cabinet's approval to regulate the cybersecurity ecosystem and ratification of the Budapest and Malabo Conventions which has enforced the country's cybercrime fight through international cooperation. On awareness creation efforts, the “A Safer Digital Ghana” campaign in collaboration with UNICEF Ghana has achieved a number of important milestones. The campaign has led to the education of over 47,500 school children nationwide on cyber hygiene best practice procedures. As a responsive approach to cyber-related incidents, the Cybercrime/Cybersecurity Incident Reporting Points of contact which was

launched by the Minister for Communications during the formal launch of the 2019 edition of the NCSAM has facilitated the mitigation of a number of cybercrime cases and cybersecurity incidents. The launch of the Child Online Protection (COP) reporting portal will be another significant milestone in addition to our modest achievements, he indicated. The intervention will help in blocking, filtering and taking down illegal/illicit content pertaining to children and young people's activities online. He additionally lauded the Internet Watch Foundation (IWF) for the collaborative effort. Although a lot of efforts has been achieved in the area of COP with the development of the National COP Framework serving as a guideline requirement to regulate COP related activities, the portal will augment the country's achievements in the area, he asserted.

On the state of preparedness of the country's cybersecurity, the National Cybersecurity Advisor indicated that the International Telecommunication Union (ITU) according to its Global Cybersecurity Index (GCI) score projected Ghana's previous rating from 32.6% in 2017 to 43.7% in 2018. This score is anticipated to rise further to over 50% in 2020 considering the investments and initiatives implemented in the cybersecurity ecosystem within the past 2 years. The strides made in cybersecurity development has gained Ghana recognition internationally with the Council of Europe, the World Bank, UNICEF, ECOWAS Commission, African Union (AU) and the ITU, which has projected the country as a leader in cybersecurity on the continent, particularly within the sub-region, he disclosed.

The Advisor lauded the President for demonstrating such a strong political commitment to the cybersecurity agenda through his dedication to lead the national cybersecurity efforts by gracing the NCSAM event for two consecutive years (2017 -2018). He also commended the Minister for Communications for her relentless effort and hard work in the cybersecurity discourse. "The NCSAM will consolidate our formal and informal cooperation into building a secured digital ecosystem", he concluded.

"The launch of the Child Online Protection (COP) Reporting Portal will be another significant milestone in addition to our modest achievements as the intervention will help in blocking, filtering and takedown of illegal/illicit content pertaining to children and young people's activities online."



Madam Anne-Claire DUFAY

Country Representative, UNICEF Ghana

Remarks

The Country Representative of UNICEF Ghana, Ms. Anne-Claire Dufay in her remark, deemed the event as a great occasion which UNICEF Ghana was very much pleased to be associated with, considering the priority placed on children's safety on the internet which is reflected by the launch of the COP reporting portal. She considered the initiative as a key intervention to help address the numerous challenges children encounter in their use of the internet. The Country Representative of UNICEF Ghana presented statistics to buttress the point that children and young people constitute the majority of digital citizens and due to their naive and vulnerable nature, their risk of exposure to violence and illicit content online is high, hence, their safety must be of grave concern to all key stakeholders. UNICEF recorded

7,000 cases in online child sexual exploitation and abuse (OCSEA) in 2019 as compared to the 750 cases in 2016, she further pointed.

She commended the Government of Ghana for the pace of progress on the country's cybersecurity development witnessed over the past three and half years whilst applauding the collaborative efforts between UNICEF Ghana, Ministry of Communications, the National Cyber Security Centre and the Ghana Police Service to curb the menace of child online abuses and exploitation. She added that Ghana is among 43 countries worldwide partnering with the Internet Watch Foundation (IWF) on this initiative which will complement the existing incident reporting points of contact and facilitate the removal of child obscene material online through international cooperation.

Associating the COP reporting portal

to another major intervention, she indicated that a Digital Forensics Lab was established at the Criminal Investigations Department (CID), adding that she considered these key initiatives as ones that will augment the mechanisms for addressing child online issues and commended Ghana on being a game-changer in child online protection. With regards to other collaborations, she disclosed that UNICEF Ghana was working with the Ministry of Education and the Ghana Education Service to integrate the concept of COP into the curricula of all levels of education in the country and expressed appreciation, for the nationwide cybercrime/cybersecurity sensitisation programme which has engaged over 47,500 students.

In concluding, Ms. Dufay requested the Government to operationalise the protocols for the Convention on the Rights of the Child to strengthen the COP efforts on children's inclusiveness online.



Mr. Christopher LAMORA

Deputy Chief of Mission/Chargé D'Affaires, U.S. Embassy Ghana

Remarks

The Charge D'Affaires/ Deputy Chief of Mission at the United States Embassy in Ghana expressed his delight to represent the US Government to participate in the National Cyber Security Awareness Month (NCSAM) 2020 event. He elaborated on the excellent collaboration the US Government has with the Government of Ghana as part of the Security Governance Initiative (SGI) aimed at improving the effectiveness of Ghana's security sector in cyber, maritime and physical border. The collaborations, he said will help improve the fight against cybercrime and the securing of Ghana's maritime border initiative as well.

The phenomenal advances of ICT over the past decade have necessitated the need for this conversation because technology has presented numerous

opportunities and has also permitted the influx of malicious actors, he indicated. Digital technology and connectivity are critical to daily life hence some measures must be implemented to mitigate the operations of internet predators who seek to exploit vulnerabilities especially with Ghana coming of age in technological advancements. He also commended the effort by the National Cyber Security Centre and the Criminal Investigations Department (CID) in apprehending the administrator of the notorious pornographic website, *EmpressLeaks*.

The Charge D'Affaires/ Deputy Chief of Mission further indicated that the SGI has championed inter-agency and inter-ministerial cooperation which highlights a lot of benefit in cybersecurity including the relentless effort in staying one step ahead of cybercriminals through devising incident response mechanisms.

He added that the United States of America has taken a cue from the NCSAM programme and is launching its own awareness month campaign themed *"Do your part by being smart"*. Mr. Lamora ended by indicating that the United States Government was honoured to partner with Ghana in awareness creation through the SGI which is evidenced in the multi-stakeholder approach adopted in the country's cybersecurity development.



Hon. Cynthia Mamle MORRISON

Minister for Gender, Children and Social Protection

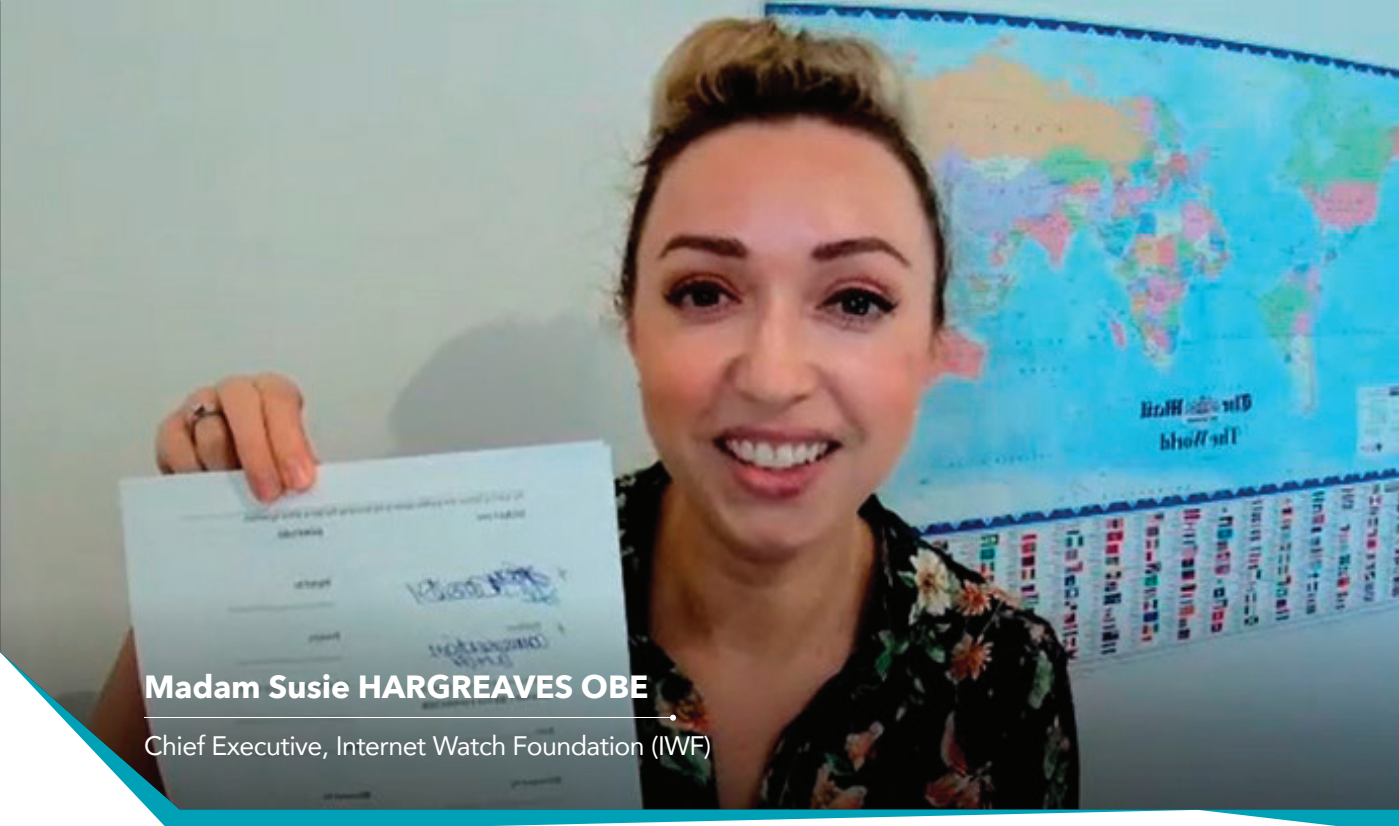
Remarks

The Minister for Gender, Children and Social Protection (MoGCSP), Hon. Morrison in her opening remarks deemed it an honour to be part of the event especially because COP issues remain a paramount interest. She acknowledged that the theme for the NCSAM was appropriate for the month-long event considering the current circumstances as it would help develop pragmatic solutions to the dangers confronting children online. She indicated that children rely on digital solutions for a lot of activities that sustain their daily lives even though it also remains an avenue to destroy their livelihood. For instance, the COVID-19 pandemic has introduced younger children to digitally designed tools for the first time and due to their naivety and vulnerable nature, they

are easily exposed to and targeted by online predators putting them at greater risks to online harms such as cyberbullying, sexual exploitation, exposure of illicit content, among others.

The Minister expressed the delight of MoGCSP to be associated with the NCSAM which is aimed at strengthening the COP agenda while commending the newly launched COP Reporting Portal as a landmark initiative to strengthen the right of children online. She declared the collaborative efforts from the Ministries, Departments and Agencies (MDAs), the media and private sector stakeholders as encouraging and thanked them for their immense support especially UNICEF Ghana for their relentless and immense effort in the Ghana Against Child Abuse (GACA) initiative to support children safety online. In

concluding, she urged children to stay SMART online by observing the best cyber hygiene protocols and recommended that the country's effort should not be relinquished until children are entirely safe online.



Madam Susie HARGREAVES OBE

Chief Executive, Internet Watch Foundation (IWF)

REMARK & SIGNING OF COP REPORTING PORTAL CONTRACT: INTERNET WATCH FOUNDATION (IWF)

In a video production, Madam Susie Hargreaves OBE, Chief Executive of the Internet Watch Foundation (IWF) expressed her delight to represent the Foundation to celebrate the signing of Ghana's COP Reporting Portal contract while lauding the stakeholders present for their commitment to safeguarding children online. She indicated that the portal is more than a reporting mechanism but also serves as a symbol of action for a country, a symbol of how the people of a country regard the importance of children and a symbol of digital

citizenship and prosperity. Madam Susie Hargreaves OBE then added that it is the responsibility of a community and a country to raise a child and to keep people safe. She expressed her gratitude to the Minister for Communications as well as the Ministry for supporting the COP reporting portal project and the National Cyber Security Centre (NCSC) for enabling the launch of the COP Reporting Portal. "The IWF further appreciate UNICEF-Ghana for their ongoing support and for facilitating the cooperation between the Foundation and the Government of Ghana. For the stakeholders present, thank you for demonstrating the commitment and support to this milestone which signifies a key step to joining the global community of countries which provide a way for their citizens to report criminal imagery of children being sexually abused" she added.

She disclosed that the mission of the IWF is to identify and remove all kinds of abusive online imagery pertaining to children including building technologies and providing services so that internet companies across the world can keep their customers safe. In highlighting the Foundation's mission with the current pandemic situation, she indicated that the COVID-19 pandemic has brought a surge in child-related criminal images and videos online thereby accounting for a 50% increase of reports from the public over the past few weeks and months via the IWF hotline. Technology has again demonstrated to be imperative to sustainable socio-economic development and progress even in the outbreak of the pandemic. Technology has made it possible for signing the COP reporting portal contract without being physically present despite the

initial desire and intention of the Foundation to be physically present for the occasion, demonstrating the relevance of technology as a crucial component of people's daily lives.

"The key element of the success of a COP reporting portal is to ensure that citizens know that there is a mechanism for making reports on these types of criminal imageries. Awareness-raising on the issues of online images and videos of child sexual abuse requires constant effort and despite the IWF running a reporting solution for the past 24 years, the Foundation prioritises Awareness Creation" she said.

She then signed the COP reporting portal contract to mark Ghana as the 43rd country in the IWF's reporting portal launch. She concluded by thanking the Government of Ghana for its proactive stance in fighting child sexual abuse imagery online.

"The IWF further appreciates UNICEF-Ghana for their ongoing support and for facilitating the cooperation between the Foundation and the Government of Ghana. For the stakeholders present, thank you for demonstrating commitment and support to this milestone which signifies a key step to joining the global community of countries that provide a way for their citizens to report criminal imagery of children being sexually abused"



Keynote Address

Hon. Ursula OWUSU-EKUFUL

Minister for Communications (Address delivered by **Hon. Alexander K. K. Abban**)

OFFICIAL LAUNCH OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2020 & LAUNCH OF THE CHILD ONLINE PROTECTION REPORTING PORTAL

In a keynote address delivered on behalf of the Minister for Communications, Hon. Ursula Owusu-Ekuful, the Deputy Minister for Communications, Hon. Alexander K.K. Abban noted a number of priority and strategic investments and initiatives being implemented in Ghana's cybersecurity ecosystem as well as the multi-stakeholder and collaborative approach to cybersecurity development,

resulting in the country earning an enviable partnership with the IWF for the launch of the 43rd COP Reporting Portal. Hon Alexander K.K. Abban delivered the keynote address stating that;

It is my esteemed privilege to welcome all of you to this year's edition of Ghana's National Cyber Security Awareness Month, themed "Cybersecurity in the Era of COVID-19". Hosting this event for the 4th consecutive time, starting in 2017 as a week-long event, is a feat I am proud to be associated with. Our overarching theme for this year's event has been appropriately chosen to reflect the times we are in.

I believe by now we have ascertained that the utilisation of the internet has become an integral part of our everyday lives, more so that of young people. Research from an ITU and UNESCO 2019 report launched by the Broadband Commission for

Sustainable Development Goals, posits that more than 50% of the world's population is now online, whereas children constitute more than 30% of Internet users. By 2022, another 1.2 billion new users would have been added to this figure, with children being the fastest-growing online demographic. Evidently, the continuous reliance on the internet by people and nations around the world has become conspicuous over time. The advent of the COVID-19 pandemic have further demonstrated how increasingly dependent governments, private sectors and individuals are on technology. Indeed, reliance on ICT and the internet has led to immeasurable opportunities for citizens, especially children and young people who rely on the internet to conduct research, attend classes, study, and socialise, among others. Ladies and Gentlemen, the theme for this year's event – Cybersecurity in the Era of

COVID-19 is reflective enough considering the circumstances we find ourselves in where digital infrastructure has become the bedrock of our socio-economic development. In view of this new reality, cybersecurity across all sectors has become imperative.

Ghana has already begun the process to secure its digital journey and a number of initiatives have been implemented over the past 3 and half years of my stewardship as the Minister with oversight responsibility for cybersecurity matters. Ghana launched the Safer Digital Ghana campaign in 2018 to create awareness among Children, the Public, Businesses and the Government. Ghana has also ratified two important international treaties on cybercrime and cybersecurity – the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, and the Convention on Cybercrime, also known as the Budapest Convention. Ghana has also revised its National Cybersecurity Policy & Strategy and I intend to submit this document to Cabinet for consideration before the end of the year. My Ministry, through the National Cyber Security Centre (NCSC), has also revised the National Child Online Protection (COP) Framework which has enhanced our preventive and reactive interventions in addressing child online safety issues. To further improve the regulatory regime for cybersecurity, my Ministry has submitted a draft Cybersecurity Bill to Cabinet for consideration. Parliament is expected to consider this Bill before the end of the year. Ladies and Gentlemen, our work on cybersecurity at the domestic level has won admiration and commendation from the international community. The Council of Europe has recognised Ghana as the hub for cybercrime capacity building in the English-speaking ECOWAS region. The World Bank has praised Ghana's formative developments in cybersecurity and has provided support to consolidate our modest gains. The World Economic Forum has identified Ghana for a public-private sector partnership on cybersecurity. In February 2020, Ghana hosted

the 8th Annual Freedom Online Conference which brought together over 300 participants from 60 countries across the globe to engage in discussions around cybersecurity and digital rights. With Ghana at the helm, the Conference placed emphasis on reviewing the current state of digital rights across Africa, as well as outlining strategies for improving digital rights on the continent and globally. During this event, Ghana, together with the Government of Germany launched the Digital Inclusion statement which has been adopted by FOC countries. Ghana has made great strides in contributing to the global response to cybercrime and we will continue to do so. In June this year, Ghana was nominated to serve on the Independent Advisory Committee (IAC) of the Global Internet Forum on Counter-Terrorism (GIFCT). Ghana's nomination to serve on the IAC of the GIFCT is another avenue to continue its sub-regional leadership role in improving cybersecurity across the globe. Ghana has also participated in a number of United Nations consultative processes on cybersecurity. One major achievement over the last year has been the successes that have emanated as a result of the launch of the Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC). Exactly a year ago, I launched the PoC to facilitate the reporting of cybercrime and cybersecurity incidents by the public. Since the operationalisation of the PoC, the NCSC has received countless cybercrime/cybersecurity incidents from the public. Key among these reports are online fraud, publication of non-consensual intimate images (sextortion), online impersonation, malware attacks, online blackmail, website defacement, among others. Cumulatively, a total of 11,545 reports have been made through the PoC between January and August 2020. Interestingly, a significant number of people called the NCSC through the PoC to seek guidance and direction in resolving cybersecurity incidents. Ladies and Gentlemen, the arrest and the ongoing prosecution of the mastermind of the Empressleaks website is a direct result of the launch of the PoC. As mentioned

earlier, children and young people make up a significant percentage of internet users. Hence, in spite of some of these advantages mentioned, the utilisation of the internet has led to children and young people becoming more and more threatened by Child Sexual Abuse Materials (CSAM), whereby children are exposed to online sexual abuse through cyber grooming, cyberstalking, sexting, commercials and gaming applications. That is why the 2020 NCSAM launch is being done in tandem with the launch of the Child Online Protection (COP) Reporting Portal. The Child Online Protection reporting portal will be used to receive reports of CSAM available on the internet. This can enable reporting of cases to the appropriate organisations such as Facebook, to ensure that the images are taken down. The portal, which will complement the PoC will provide a safe platform for people to report suspected child sexual abuse materials. It is my firm belief that the National CERT will find the collaboration with the IWF beneficial in responding to cybersecurity incidents involving children. Ladies and Gentlemen, the NCSC has adopted a hybrid approach of delivering this year's awareness campaign by combining both physical interactions, under strict COVID-19 protocols, and the use of available virtual platforms. A number of activities are planned for the month including the Launch of the Security Operations Centre (SOC) at the National Information Technology Agency (NITA), Cybersecurity Roundtable Forum on the Impact of COVID-19 on Ghana's Digitalisation Agenda, Cybersecurity Forum with Industry Players, Joint Freedom Online Coalition (FOC) programme on Digital Inclusion, Joint engagements with SEI/ MITRE through the Security Governance Initiative (SGI), Council of Europe Workshop on Cybercrime & Electronic Evidence Handling for Criminal Justice Sector, Regional Cybersecurity Capacity & Sensitisation Programme among others. In addition, there will be public engagements with children and parents on Cyber Hygiene best practices. There will also be a live broadcast of selected events including a Cybersecurity Workshop on

Mobile Money Fraud, through social platforms and media outlets. The need for this is as a result of the wider population's dependency on digital platform, hence the NCSC through the Ministry of Communications (MoC) will leverage this development to intensify capacity building and awareness creation efforts. This will in turn equip citizens with the risks associated with these perilous times and the countermeasures they can put in place. Most importantly, the event will go on to highlight what the Government has achieved in the area of cybersecurity within the past three and half years. I hope you carefully look through the programme outline, identify the events that fall within your scope and participate actively in them. I wish to express my appreciation to UNICEF, the Council of Europe, the World Bank, the United States government and all our partners in supporting our journey to secure Ghana's digital development. In conclusion, I believe that the purpose of this gathering will continue to reaffirm the Government's commitment to building a secure cyber ecosystem. On that note, I officially declare the 2020 edition of the National Cyber Security Awareness Month and the COP reporting portal to support child online protection efforts launched.

The event saw about 500 views via the Youtube Channel of its media partner CITI FM as well as over three (3) thousand views via Yen.com. 300 hundred participants were physically present for the first day of the COP week.

"Media interviews were conducted with key speakers at the event at the close of the event."

WEEK ONE

CHILD ONLINE PROTECTION



CYBERSECURITY
IN THE ERA OF
COVID-19



NATIONAL
CYBER SECURITY
AWARENESS MONTH

CHILD ONLINE PROTECTION WORKSHOP FOR TELECOMMUNICATION SERVICE PROVIDERS



As part of the National Cyber Security Awareness Month (NCSAM) 2020, the National Cyber Security Centre hosted a workshop for telecommunication service providers to discuss the present state of Telecommunication Service Providers and other related organisations in combating child online sexual exploitation and its related matters. In attendance were the Deputy Director-General for the National Communications Authority (NCA), Madam Olivia Quartey, the Chief of Child Protection for UNICEF Ghana, Mr. Muhammad Rafiq Khan, the Head of Cybercrime Unit of the Criminal Investigations Department, Dr. Gustav H. Yankson, dignitaries and stakeholders from government institutions and civil society organisations.

Welcome Remarks

Fredrick KWAKYE-MAAFO

Lead Critical Information Infrastructure, NCSC

Mr. Kwakyee-Mafo formally welcomed the dignitaries and all organisations present, highlighting the purpose of the workshop.

Purpose for Gathering

In his pre-recorded welcome speech, the National Cybersecurity Advisor addressed the reason for the COP Workshop which was to discuss the threats children and young people face as they are exposed to and have access to the internet. He added that he hoped that parties at the workshop engage, debate and discuss the way forward.





Keynote Speech

Madam Olivia QUARTEY

Deputy Director-General - National Communications Authority

Madam Olivia Quarthey in her speech recognised the work of the Ministry of Communications (MOC) and the National Cyber Security Centre in making child online protection a key focus in Ghana's Digital Agenda. She also noted the collaboration with Ghana's international partners such as the Internet Watch Foundation (IWF) in helping make the internet a safer place for the children of Ghana. Madam Quarthey lauded measures undertaken by the Government of Ghana to protect citizens, especially in the COVID-19 pandemic era. As online platforms had become essential to create some sense of normalcy, there were some dangers still lurking on the internet and since the onset of the COVID-19 pandemic, cyber threats have intensified, as malicious persons have taken advantage of the pandemic.

She referred to the following cyber-related reports: (1) A 2020 ITU news brief that indicates that Tech companies have seen a spike in phishing traffic of up to 300 per cent across their networks; (2) The Global Status Report on preventing violence against children, jointly published by WHO, UNICEF and other stakeholders released in June 2020, recorded an increase in harmful online behaviours including cyberbullying, risky online behaviour and sexual exploitation as online communities have become central to maintaining many children's learning, support and play.

Madam Olivia Quarthey also noted the effects children exposed to violence suffer which included drug and alcohol abuse, depression, mental health problems as well

as criminal behaviours as adults, whilst emphasising the key role policymakers and practitioners have to play in protecting the best interests of future leaders.

Child Online Protection (COP) was established by the International Telecommunication Union in 2008 and is an international collaborative network to protect children worldwide against cyber threats by providing legal, technical and organisational measures. She spoke on the 2020 Guidelines on Child Online Protection for teachers, parents and the industry. These guidelines she noted, hold a wealth of information on how to develop a safe and empowering online environment for children and young people.

She described the response of industry players to the Government's call for support at the onset of the COVID-19 pandemic as favourable indicating that telecommunication operators, provided zero-rate for educational websites, several medical information portals and several government portals were offered at low or no rates to customers.

She then called on the telecommunication operators to yet again, lend their support to the protection of children whilst online so that the digital space does not present adverse effects on the development of children. According to her, the NCA is very hopeful that industry players, civil societies, and the general public will heed this call. Touching on the successful launch of the Child Online Protection Reporting Portal, she expressed her gratitude, that victims of child online sexual abuse and exploitation now have a dedicated channel to report and seek support. She explained that the National Cyber Security Centre - Computer Emergency Response Team and other sectoral incidents response community, which involves the Mobile Network Operators, should be leveraged along with the newly launched portal for expeditious support.

Remarks

Mr. Rafiq Muhammad KHAN
Chief of Child Protection, UNICEF Ghana

In his welcome remarks, Mr. Khan reiterated the importance of the internet and Information Communication Technology in the lives of children, especially during the COVID- 19 era as more children are spending increased time online, in Ghana and all around the world.

He referred to some statistics in Ghana on mobile phone and internet usage. He noted an increase from 19 million mobile phone subscribers in 2017, to around 20 million in



2020. Internet users have also increased from 8 million mobile internet users in 2017 to about 15 million users.

He indicated that the US National Centre for Missing and Exploited Children (NCMEC), mandates all USA telecommunications companies (Google, Microsoft) to report online child sexual materials, and are, by law, bound to remove all the known child sexual materials on websites, servers or any infrastructure. These companies are also bound to report where that data is being uploaded from or accessed or being transferred.

This is specifically based on the known tactics such as photo DNA software. These are scanned and reported to the NCMEC. In 2016, there were 750 reported cases on people who were accessing or viewing or transferring child sexual material because it is based on the IP address. In 2019, that number rose to 7,000.

To make cyberspace a safe place, UNICEF in collaboration with the International Telecommunication Union at the UN level developed a Child Online Protection

Framework. He noted that there are a set of guidelines for the industry, i.e. Telecommunication service providers. What it presents is how to establish a common draft response and guidance to ICT and online industries and relevant stakeholders; it provides guidance to companies on identifying, preventing and mitigating, any adverse impacts of their products and services on children's rights. It also provides guidance to companies on identifying ways in which they can promote children's rights and responsible digital citizenship among children. It also suggests common principle to form the basis of national and regional commitment across related industries, while recognising that different types of businesses will use diverse implementation tools. The first edition of these guidelines came out in 2016 but have since been revised.

He acknowledged that some of the present ICT and Telecommunication companies, already have due diligence policies in place, and some have already signed the COP Framework with UNICEF. He requested working with these companies to assess how their services are helping children to reach their full potential, and if there are any risks or lapses in their services, how then can they overcome these problems. He spoke about UNICEF's Child Online Assessment Tool, which empowers technology companies to promote a safe online environment for children. He noted that UNICEF would be happy to work with these companies, in collaboration

with the NCA and the NCSC, in an objective manner and see where improvements can be made. For this, UNICEF will be happy to set aside some resources to ensure successful implementation. The primary objective of the tool, he describes, is to ensure companies understand the core issues and impacts to consider when assessing their management of child rights and the internet. It offers an easy-to-use and comprehensive self-assessment of the company's management as well as the impact on children. The tool uncovers strengths and weaknesses in managing children's rights policies and practices, and build 'proactive' plans where needed.



Presentation

Madam Lawuratu MUSAH-SAAKA Child Online Protection Lead, NCSC

The presentation on Child Online Protection began with Madam Lawuratu Musah-Saaka projecting some statistics. She gave a background on COP indicating that the ITU has been the main driver of COP, having started in 2007, with the Cyber Security Agenda & the Child Online Protection Initiative with UNICEF in 2002. At the time, she noted, the COP Initiative was to focus on cybersecurity issues with children and young people, in accordance with the Convention on the Rights of the Child, and the Sustainable Development Goals (SDGs). She spoke on the National Child Online Protection Framework, which was put together by the Government, through the Ministry of Communications. She further indicated the 5 pillars on which the Framework was based which are legal measures, technical and procedural measures, organisation

structure, capacity building and international protection. At the Abu Dhabi Summit in 2015, Governments & organisations guided by the Model National Response (MNR), agreed to establish and deliver a coordinated national response to online child sexual exploitation in their own countries. Subsequently, the MNR was developed to provide states and organisations with guidance and support to help them fulfil this commitment. The WePROTECT Global National Alliance Model National Response (MNR), mean that nations could adapt it to suit specific national situations. Ghana, as a member of WePROTECT Global Alliance, took it up. The model, she noted, has 6 capabilities with 21 sub-capabilities. For the purpose of this workshop, the focus was on Industry capability. The sub-capabilities under this include:

(1) Notice and Takedown Procedures
(2) Child Sexual Exploitation and Abuse reporting
(3) Innovative Solution Development
(4) Corporate Social Responsibility
(5) Framework Validation.

She also noted the ITU 2020 launch of Guidelines for Industry, which was done in partnership with UNICEF. Under this, she elaborated on the sections, which include the following:

(1) Identifying, reporting and mitigating. The Guideline talks about child protection and safeguarding policy, or integrating specific risks and opportunity pertaining to children and young people's rights into company-wide policy commitments. Another section deals with

(2) identifying child rights impacts on different age groups as a result of company operations (3) adopting empowerment and education-based approach to child protection especially to consider data protection rights, their right to privacy and freedom of speech, while offering education and guidance through company services. (4) Industry collaboration with government, law enforcement, civil society, and hotline organisations by prohibiting, the uploading, posting, sharing or transferring or making available content that violates the rights of any party or infringes any local State's national or international law.

(5) To include, greater emphasis on data retention and preservation as well policies to support law enforcement in the event of criminal investigations. It also provides that the industry can help create a safer digital environment for children and young people, by adopting safety and privacy by design principles in companies' technologies, and present information to children regarding the rules of a site in an appropriate, accessible and detailed manner. Service providers should educate customers on managing concerns related to internet use- spams, data theft and inappropriate contacts e.g. bullying.

SESSION 2

Roundtable Discussion on COP



Focal area- How Child Online Protection Guidelines can be integrated into policies and management. Questions were presented by the NCSC for discussion:

Q1

What are some adequate measures that have been taken by organisations to identify, prevent and mitigate potential & adverse impact on children's right (already existing initiatives)

Responses

The representative from MTN Ghana indicated that the company had collaborated with organisations such as UNICEF in streamlining online pornographic sites and attempting to block such sites.

Curious Minds, a youth led organisation added that as an organisation, they educate the

youth on online safety tips and some cybersecurity issues. They partner with Child Online Africa (which also focuses on educating and informing the youth about safety tips). AirtelTigo Ghana also noted that it runs awareness campaigns throughout the organisation annually, and the year 2020, focus was on COP. Additionally, they requested to know the guidelines to follow and concluded that they seek consent from parents or guardians before interacting with children on the matter.

Ghana Scouts Association indicated that they rely solely on the National Communications Authority (NCA) for all COP related protection protocols. The National Commission for Civic Education (NCCE) also indicated that since 2018, the commission has served on several committees for the National Cyber Security Awareness Months and has been able to gather

materials to constantly remind organisers on the importance of COP (and includes COP and cybersecurity materials in their quarterly programme guide). Africa Online Ghana has been able to identify and resolve malicious attacks. The Ghana Maritime Authority noted that, in collaboration with the National Information Technology Agency (NITA), the Authority has tried to filter all unnecessary and unrelated sites within their organisation. Representatives from InfoTech Solutions indicated that they run services on systems basis; educate caregivers and parents, as they observed high interests of children in the use of the internet.

The NCA noted that, as a member of the National Cyber Security Technical Working Group (NCSTWG), it has supported in developing appropriate policies and framework that have especially focused on COP.

The NCA itself focuses on educating consumers on COP. The Authority also has a Computer Emergency Response Team (NCA-CERT), which gathers reports on vulnerabilities and incidents. This information is shared with related agencies to address and put in place the necessary measures to prevent a repetition of such incidents. The representative for the NCA, Mrs. Jennifer Mensah further went on to indicate that a newsletter for educating consumers with a specific aspect on COP has also been developed.

The Criminal Investigations Department (CID) in stating their role indicated that a number of investigations on cybersecurity breaches have taken place. According to ACP Dr. Gustav H. Yankson, the CID does digital forensic investigations, meaning that they are able to extract deleted information from digital devices. They also undertake a lot of awareness creation and education. He stressed the need, however, to do more sensitisation and his expectations of the Telecommunication Service Providers was for them to do more to assist law enforcement agencies, seeing as the evidence can be traced via their systems. Dr. Yankson also noted that service providers, should be able to provide IP information to assist in investigations, but they fall short in this regard. In his closing remarks on that topic, he stressed the need for service providers to keep records of IP addresses. Additionally, the CID, he indicated, assisted the NCSC with the COP Framework, and liaised with the NCSC on Cybercrime/ Cybersecurity Incident Reporting

Points of Contact, in addition to receiving cases from the NCSC. He indicated that the CID also works with UNICEF on child online-related issues. He spoke on the need to work on parents/ guardians as it has been observed that young people and children are afraid to share challenges with parents.

Madam Musah-Saaka added that there was the need to put more efforts into awareness creation adding that one key mandate of the NCSC is awareness creation & capacity building.

There was however the need to set up training for the other regions.

Globacom added that there has been established a dedicated team of 2 members of staff to handle COP related issues with COMSYS Ghana Limited noting that their major focus has not been child protection in cyberspace but rather to provide effective services and ensure secured systems. The representative highlighted that the Telecommunication providers do not have control over social media platforms eg WhatsApp, Facebook and cautioned that this should be an awakening and awareness for these Service Providers.

Dr. Yankson noted that the focus of Service Providers is first, to make a profit and so it was up to the NCA to ensure that Telecommunication providers are protecting their consumers. These entities being the ones to provide access to online and social media platforms reaffirms the benefit they will provide in keeping IPs. This falls under their Corporate Social Responsibility (CSR).

Q2

Is there a dedicated team in institutions responsible for COP or is it a day-to-day activity & do they have access to the necessary stakeholders?

Responses

The CID made known that there were currently 1000 investigators who have been trained and there, are still more people being trained.



The representative from Internet Solutions made known that they do not have a specific team assigned to COP but that it falls under the cyber team's responsibility. Additionally, he does not think it is right to stalk consumers online. Being an internet service provider, he stated it is difficult to prevent COP perpetrators. Thus, they rely heavily on third-party reports.

In response, Mr. Khan spoke on tools being used globally, which Internet Solutions can also use, to safeguard customers. He also spoke on the use of the Content Moderator tool (a software which filters images or words used on Facebook). In his closing remarks, he stressed that when it comes to COP, there is no difference of opinion, privacy is secondary.

Madam Audrey Mnisi-Mireku of the NCSC also responded by saying there is no law that mandates telecommunication operators to ensure COP, but they are to follow and comply with local laws. Therefore, if Ghana has signed any treaty or law, all relevant parties are bound to it.

Closing Remarks

Madam Lawuratu MUSAH-SAAKA NCSC

In conclusion, the COP Lead of the National Cyber Security Centre stated that the NCSC through the NCA would send out risk assessment tools to the telecommunication operators to use and provide a report on, to which all organisations present agreed to.

CYBER HYGIENE BEST PRACTICES FOR SCHOOL CHILDREN



The National Cyber Security Awareness Month (NCSAM) 2020, also had the National Cyber Security Centre organise an event targeted at educating children and young ones and equipping them to be safe online. Partnering organisations and stakeholders attended to shed more light on the topic. This broadcasted event was intended to reach all parts of the world, especially our target groups. The programme was adequately attended by dignitaries and stakeholders from government institutions, civil society groups, academia, and school children from selected schools. The event saw the participation of over 200 people physically as well as 300 hundred views on Citi FM's (a key media partner) Youtube Channel with about 7000 views on the Facebook page of Yen.com.

Welcome Address

Dr. Albert ANTWI-BOASIAGO
National Cybersecurity Advisor

In his welcome address, Dr. Albert Antwi-Boasiako, the National Cybersecurity Advisor noted how important child online protection is to the Ministry of Communications, and steps taken by the Ministry,



through the National Cyber Security Centre (NCSC) together with its partners has helped deal with the challenges faced in the focal area. He indicated some of the dangers that can be experienced on the internet in the kind of content posted, contacts established, and conducts of children themselves. He indicated that the purpose of the event was to share basic cyber hygiene best practices that can be adhered to while enjoying digitisation. He referred to some statistics including a survey conducted by UNICEF in about twenty-five countries, where about 82% of children are at risk of being exposed to sexual images on the internet. He spoke on the operation conducted by the NCSC, together with the Criminal Investigations Department (CID), in which he described how the administrator behind one of the notorious websites that hosted

such information was arrested. He showed great appreciation to UNICEF for their efforts and dedication in working with the NCSC for the past three years. In his closing remarks, he identified some social risks children face from the internet, and how important it is for parents to build trust with their children to help address some of the issues faced.

Remarks

Mrs Joyce ODAME
Child Protection Officer,
UNICEF Ghana

Madam Joyce Odame in her remarks noted that in an increasingly digitised era and the phase of COVID-19, the internet is used for all engagements, hence the need to ensure a safe and conducive environment for children. She identified some benefits children get from the internet such as playing and learning. She however noted that although the internet and these technologies provide unparalleled opportunities for children and



young people, the growth in the use of the internet and its widespread availability and accessibility within the nation may pose challenges. According to her, the internet may undermine the rights of children, because as more children gain access to the internet, the risks of experiencing abuse and exploitation have become an unfortunate reality. She highlighted the importance of collective responsibility, including that of children and young people, to ensure that the digital environment is safe for everyone. She pointed out ways to ensure safety in the digital environment, such as being responsible in the way the internet is used, being active in ensuring our own protection, and demonstrating good digital citizenship while online. In her closing remarks, she explained that UNICEF will continue to support the government and relevant stakeholders to ensure that children are empowered to ensure that they participate meaningfully in the digital space, and be protected, whether online or offline.

Poetry Recital

The poetry recital given by Miss Enam Galley touched on the impact of COVID-19, the works of the NCSC in digitisation, the interest and curiosity of young people on the internet; the benefits the internet has provided such as online classrooms and studying, the NCSC measures to ensure that child online protection is firm to protect children from the dangers online as well as being dangers to others, not giving



in to online threats and reaching out to the NCSC through available channels of the Cybercrime/Cybersecurity Incident Reporting Points of Contact (POC).

Remarks

Mr. Christian Kwasi MAWUSI
Principal Programmes Officer,
Ministry of Gender, Children and
Social Protection (MoGCSP)



The Principal Programmes Officer at the Ministry of Gender, Children and Social Protection, Mr. Christian Kwasi Mawusi, noted the delicate nature of



COP, which is why it is an area, which causes an alarm for all stakeholders. He added that there was a need for awareness creation on good cyber hygiene protocols. He noted how the internet has become an important part of lives, and how this has exposed children to perpetrators, who take advantage of their vulnerability and abuse them online. He spoke on the matter of sextortion indicating that, it has become one of the most recorded crimes in the country as a result of unsupervised use of the internet by children and young people. He advised that young people need to be careful with what they share online because the internet does not forget. He encouraged them to stay 'SMART' online and hoped that the campaign to strengthen Ghana's cybersecurity and raise awareness on cybercrime, especially on COP, would go far and gain prominence.

Drama Display

Pupils of Wisdom Ways Academy

The drama presentation focused on common cyber threats children and young people face in this modern age. The drama centred on a young girl who had taken intimate pictures of herself, which a cybercriminal had gotten hold of and used to blackmail her parents to obtain some money.

The drama also touched on the need for parents to stay informed and develop good relationships with their children. It encouraged the use of available channels of the NCSAM which is the Cybercrime/Cybersecurity Incident Reporting Points of Contact for the reporting of incidents.

A woman wearing a blue and yellow patterned headwrap, glasses, and a white face mask is speaking into a microphone at a wooden podium. Behind her is a large screen displaying a presentation slide with the Ghanaian coat of arms and text about a national cyber security awareness month. The slide lists two points: 'A National campaign of the National Cyber Security Centre was launched by the V... 1, 2018.' and 'The programme is par... cybercrimes and cyber... improving on Ghana's... the public, business...'.

Presentation

Madam Lawuratu MUSAH-SAAKA

Child Online Protection Lead (NCSC)

CYBER HYGIENE BEST PRACTISES

Madam Lawuratu Musah-Saaka, the COP Lead at the National Cyber Security Centre, began by reiterating the importance of COP, especially for a nation that has over thirteen million of its population being children and about 57% under the age of twenty-five. She noted that the National Cyber Security Awareness Month (NCSAM) is hinged on the Safer Digital Ghana campaign, which was launched in 2018. The aim of which is to create awareness and build capacity in the four focal areas i.e Children, Public, Businesses and the Government. Noting some reports, she indicated that 10.11 million of the Ghanaian population are active internet users, with active usage of 35%, 9.28 million active mobile internet users (32%), unique mobile users being 67%. As she noted, there

is a need to be sure of the realities of a situation before introducing interventions. To that extent, the Ministry of Communications, in partnership with UNICEF conducted a survey on the risks and opportunities to children, with respect to their online practices. She presented the following: 7 out of 10 children use the internet to learn (70% active internet users). 4 out of 10 had seen sexual images at least once (40%), 2 out of 10 children had seen someone who they had met online (20%), 4 out of 10 said they did not feel safe online (40%) and 3 out of 10 also had disturbing experiences online. She referred to another poll conducted by UNICEF in New York where 1 in 3 said they had been victims of online bullying. 1 out of 5 of these children had skipped school due to online violence and bullying. She noted, that according to the UN Special Representative of the Secretary-General on the Violence against Children, 34% of respondents in sub-Saharan Africa

said they had been victims of online abuse. She spoke also on some pros of the internet such as to access information, socialisation, learning and entertainment, noting that there has been an increase in the usage of the internet in the wake of COVID-19. She referred to another set of statistics which noted that in 2019, Ghana was ranked 9th (globally) for social media usage.

She spoke on some basic terminologies, some of which she explained as some of the risks people face on the internet: cybercriminal, cybersecurity, online safety, child online abuse (cyberstalking, cyberbullying, and sextortion), profiling, child online protection, netiquette etc.

She then gave some tips for staying safe online:

- ➔ Use a strong password
- ➔ Block, report or delete
- ➔ Unfriend offensive people

- ➔ Do not give strangers access to your profile (do not accept friend requests from strangers)
- ➔ Be mindful of what you share online
- ➔ Respect other people's views
- ➔ Do not share nude photos or videos (criminal offence)
- ➔ Do not keep sexually provocative videos of yourself
- ➔ Do not meet strangers online, offline
- ➔ Do not respond to hurtful messages (cyberbullying)
- ➔ Do not share passwords or sensitive information with anyone

In her closing remarks, Madam Lawuratu Musah- Saaka spoke on the various platforms or mediums included in the PoC through which victims or people can reach the NCSC to make reports and seek assistance.

Remarks

Mr. Tony BAFFOE

Head of Information Technology,
Ministry of Education



Mr. Tony Baffoe, the Head of Information Technology, Ministry of Education began by identifying some of the ways in which the internet has helped lives and how it has connected the world. He also noted that in as

much as there are many gains and benefits, there are many challenges, such as child online grooming for sexual exploitation and a host of others. For these reasons he noted that there was the need to do a lot to protect children, as they are naturally enquiring and generally naïve, and without proper guidance succumb to the negativity on the internet. There was therefore the need to be robust in educating them, he added.

Awareness in the early stages of their lives, beyond the formal education set-up, is necessary, adding that Ghana has adopted the United Nations Safe Schools Declaration, which the Ministry of Education was in the process of putting together for a Safe Schools Policy. Some issues to be captured in this policy would be cyberbullying and online child protection. He bemoaned the failure of the Ministry's 2014 ICT policy, as it did not address these important issues. According to Mr. Tony Baffoe, ICT policy is being reviewed in this direction and the Ministry of Education is rolling out the Digital Literacy Project in schools. He ended by noting that there is still so much that can be done on the matter and he hopes that this event would provide a platform for sharing ideas on this matter.



SESSION 2

Panel Discussion with School Children

This discussion looked at some risks and opportunities that people face online. The panelists spoke on some of their personal experiences, some of which were disturbing, and the need for parents to do more supervising and getting more involved. They also spoke on ways to protect themselves and how they handled some unpleasant incidences they experienced.



CHILD ONLINE PROTECTION CYBER HYGIENE BEST PRACTICES FOR PARENTS AND GUARDIANS



The National Cyber Security Centre, through the Ministry of Communications, as part of the National Cyber Security Awareness Month (NCSAM) 2020 organised a Child Online Protection (COP) Workshop on Cyber Hygiene Best Practices for Parents and Guardians. The programme was to engage relevant stakeholders on the best practices and relevant knowledge needed to deal with children and young people using technological devices and the internet. The programme was adequately attended by representatives from the National Council of Parents Teachers Association (PTA) of Ghana, dignitaries and stakeholders from government institutions and civil society groups.



Remarks

Dr. Albert ANTWI-BOASIAKO

National Cybersecurity Advisor



According to the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako, the Ministry of Communications has identified Child Online Protection as one of the important pillars of the National Cyber Security agenda with an estimate of about 70% of school-going children using the internet. It is estimated that on a daily basis, 19% of the population use the internet. He addressed the negative aspects of the internet, such as the sharing of intimate images online. He added that the NCSC receives weekly reports of illegal contents being circulated, indicating the problem at hand. Despite all these, he noted the benefits that all can enjoy from the internet such as learning, socialisation, and entertainment. Dr. Antwi-Boasiako, in his closing remarks, identified key topics for discussion including, Parenting in the Digital Age, especially for parents who lack basic ICT skills, adding that one of the main reasons for the conversation was to identify how to ensure the devices and

activities of children online are used for the intended purposes specified by parents. For these, he explained the need to interact and discuss with the industry experts. In closing, the National Cybersecurity Advisor noted that the NCSC will be happy to take feedback to be incorporated in new developments.

Remarks

Madam Hilda MENSAH Child Protection Specialist UNICEF Ghana

Madam Hilda Mensah a Child Online Protection Specialist with UNICEF Ghana began by touching on the influencing power parents hold, explaining that parents have a lot of influence on their children especially on how they pick up after them. She spoke on how COVID-19 made it more compelling for the use of ICT and that parents needed to provide these resources to

facilitate the continuation of school online. In this regard, she stressed the responsibility of parents in supervising their children, stating how monitoring what children watch on TV and the hours spent is now a harder role. Speaking on how parents and guardians can supervise, she highlighted the issue of computer illiteracy of some parents/ guardians and how it was even the children who help with the devices and their related functionalities.

In this regard, Madam Mensah emphasised the need for all to become internet savvy indicating that illiterate and semi-literate parents were a big focus for this discussion. She ended her remarks by tasking the gathering to find ways of providing adequate content to help parents and guardians.



Remarks

Mrs Florence AYISI-QUARTEY

Ag. Director, Department of Children -
Ministry of Gender, Children & Social
Protection

The Acting Director, Department of Children, described how real cyberspace was, indicating that it was an extension of our physical world, hence, the need to guard our online presence.

She spoke on cyber hygiene- the need to stay safe and avoid exposing daily life in cyberspace. It is important, she noted, to be very careful and conscientious, adding that parents needed to educate children to know the internet is just an extension of the real world and things posted on it do not get deleted. The children, she explained, need to understand that cyber hygiene best practices are a part of daily life and not a one-time thing. For example, reading and checking what you are signing onto when online and what access is given to the devices regarding our personal information.



Remarks

Mr. Charles ADJETEY SOWAH

President, Parent Teacher Association
(PTA) Council



Mr. Charles Adjetei Sowah, the president of the PTA Council noted how COVID- 19 has made online learning more imperative due to the closure of schools. He indicated that human activities globally now depended highly on the internet and urged parents and guardians to equip themselves with the necessary knowledge to guide their wards. He further went on to provide some measures that can be adopted as follows:

- ➔ Installing security apps
- ➔ Remotely manage accounts with the ability to change parental controls
- ➔ Block access to certain web tools e.g. chat rooms
- ➔ The need to be aware of cyberbullying
- ➔ Limit the time the children and young ones spend online.
- ➔ Hide personal passwords
- ➔ A key aspect of this is building a relationship of trust with children and young ones



Presentation

Mrs Joyce ODAME Child Protection Officer, UNICEF Ghana

Mrs Odame, a Child Protection Officer of UNICEF Ghana began by describing how the internet has benefitted children and young ones. However, she noted that there are challenges faced when using the internet. She gave a statistical overview on mobile phone and internet usage particularly in Ghana, indicating that mobile phone connections in the country were more than the population (population is about 30 million) with 16 million internet users. Ghana was also within the Top 10 in global rankings on social media usage and one of the first three African countries.

She spoke on a 2016 UNICEF survey conducted on the use of the internet by children (over 2000 kids). Findings indicated that seven out of ten (7 out of 10) children use

the internet to learn and four out of ten (4 out of 10) children showed that they have seen sexual images while online. A further two out of ten (2 out of 10) said they have met someone physically they had first met online (online relationship became physical) and three out of ten (3 out of 10) children have had disturbing experiences (unpleasant encounters) when using the internet. In her presentation, she spoke on the types of risks: (1) harmful content (2) contact, explaining that people start to engage with strangers online and this progress to face-to-face contact (3) the contact of children themselves e.g. cyberbullying.

On addressing what parents or guardians and teachers can do, she indicated the following:

- ➔ Block and use controls to avoid accessing inappropriate content
- ➔ Dialogue and discussion (communicate with children and young ones)
- ➔ Get the basic information and

facts to become more familiar with ICT and the internet

- ➔ Set some ground rules e.g. hours spent online and using devices
- ➔ Friend and follow them, but do not stalk your children
- ➔ Explore with them when they are on the internet
- ➔ Install firewall and/or anti-virus on devices.
- ➔ Be a good digital role model (the grown-ups should not be slaves to ICT)

In her closing remarks, she encouraged all to be **'SMART'**.

- S** - Stay safe online
- M** - Meeting (do not meet up with people you meet online)
- A** - Accept (do not accept request from people you do not know)
- R** - Reliable (not everything you see online is credible or reliable)
- T** - Tell a trusted adult or talk to someone you trust

SESSION 2

Panel Discussion

Moderator, Madam Lawuratu MUSAH- SAAKA (NCSC)

Discussions centred on parents showing key interests in their children. To this point, the panelists agreed that, when children and young people do not receive love and affection from home, they start to seek it from other sources. This makes them vulnerable to online predators and other online criminals.

Madam Hilda Mensah re-emphasised the need for parents and guardians to be gatekeepers for their wards. The responsibility

parents and guardians to take part in the cyber world and supervise the use of devices.

Mr. Emmanuel Arthur in his remarks noted that the internet gives a lot of opportunity to young people (education, entertainment) but it also presents an opportunity for cybercrimes. He indicated that parents are not realising the signals children are giving and that there was the need to collaborate with children to fight against the threats online.

In response to how safe the internet is and what parents can do to ensure that children can still get the benefits of the internet but be safe from the threats, the panelists spoke on training children to know when to act and when not to act. Another response provided was that parents should learn about the various control measures for devices and the internet and familiarise themselves with how they work.

On the topic of why children do not report incidents to parents, it was noted that the cybercriminals put fear in the young ones to deter them from sharing their issues. A contribution from the audience on how the parents keep referring to past mistakes of their children also contributes to this. This is because it causes the child to keep their mistakes to themselves to avoid backlash. Madam Musah-Saaka raised a point that incident reports have shown that reports usually come from teenagers. One panelist's response was that what one would not do in real life, they should refrain from doing online- intimate images and sharing very private information. It was also stressed that the message on the dangers online needs to be shared and the word needs to keep reaching people.

Mr. Emmanuel Arthur, the CEO of Ramsys InfoTech Solutions asked about the effects of Facebook posts on the psychological and social status of children and young people



lies with parents and guardians to ensure that children and young people use the devices for the purpose and conditions under which they were given to them, adding that as parents supervise in the real world, so must they supervise in cyberspace. Madam Ayisi-Quartey also spoke on the dangers of parents trying to separate the real world from the cyber dimension. She encouraged

Another panelist spoke on the rural-urban dynamics, noting that parents in the rural and some urban areas lack knowledge of cyberspace but their children may be active users. Such parents, he advised, can reach out to a trusted person to play a supervisory role since the parents may not be in the best position at the time.

as the social media platforms focus on boosting interesting and engaging content. He also added that children and young people accentuate their value to the attention they get on these social media platforms as opposed to real-life which puts pressure on them to post things, they would not ordinarily do, to get more likes. The appropriate stage or age to begin teaching on cyber hygiene was also discussed where panelists indicated that once the children are seen to have some level of maturity in cyberspace, they are to be educated on what they need to know and as such there was no set age.



Parents ruin the trust built by continuously bringing up past mistakes. This pushes the children away. How can this be solved?

Response - unfortunately, parents are fond of this, but parents should not refer to past mistakes! Children do not forget, and this may cause children not come out and report to their parents.

educative program and noted that tools being used by UNICEF to engage community people on online issues should incorporate local dialects.

Madam Musah-Saaka wrapped up by reiterating the main mandate of the National Cyber Security Centre, which is to ensure awareness creation, and capacity building, hence, interested organisations in need of such education can reach out to the NCSC for assistance. Over 3.3 thousand viewers were reached via Facebook on Citi FM's page for this event.

Closing Remarks by Panelists

Questions and remarks from the audience:

Children are forced to look after



themselves, this exposes them to paedophiles and abusers who will entice these lonely children. How can the parents who leave their children to fend for themselves be educated?



Response - parents

usually do this because of high rates of poverty, so they try to create a positive image of the child in the mind of the parents. Create a 'conscientised' parent. Do not attack the parents by accusing them of being wrong but psychologically, reinforce the good/ the healthy alternative. Parents should be kind to those with whom they leave their children with as they take on the supervisory role.

Parents and guardians were encouraged to challenge children to be their own ambassadors. It was also advised that daily push (pop-up) messages should be sent to remind and inform people daily on cyber hygiene and safety tips as it would also be helpful.

It was also indicated that UNICEF Ghana and the Ghana Education Service will be rolling out a digital

LAUNCH OF DATA PROTECTION SOFTWARE AT THE PREMISES OF THE DATA PROTECTION COMMISSION



As part of the National Cyber Security Awareness Month (NCSAM) 2020, the National Cyber Security Centre and the Data Protection Commission hosted the launch of a Data Protection Software. The software is to streamline the manual processes of the Data Protection Commission and make available relevant information of the Commission. It will also make known the data controllers who are in good standing with the commission to guide consumer choices of which organisations to do business with. In attendance were officials from the National Communications Authority (NCA), Bank of Ghana, Ghana Investment Fund for Electronic Communications (GIFEC), Social Security and National Insurance Trust (SSNIT), Telecommunications Service Providers and staff of the Ministry of Communications sister agencies.

various organisations i.e., the Bank of Ghana, National Communications Authority, Ghana National Gas Company Limited and the Ghana Investment Fund of Electronic Communications that have assisted the Commission along the way. She also acknowledged the work of past board members such as the former Deputy Minister for Communications, Hon. Vincent Sowah Odotei and former employees who have helped steer the affairs of the Commission. She further went on to acknowledge the challenges faced by the DPC in maintaining its staff due to lack of resources.

Welcome Remarks

Justice Mrs Helena Inkumsah ABBAN (RTD) Board Chair - Data Protection Commission

Justice Mrs Helena Inkumsah Abban (RTD) in her remarks indicated that the Data Protection Commission has come a long way in achieving its set goals as well as the



Purpose for Gathering

The launch of the Data Protection Software is to streamline the manual processes of the Data Protection Commission to aid users to have swift and effective ways of checking on the data protection good standing of organisations in Ghana. The software is also to help data controllers register and pay fees to the commission in a timely and easy manner.



Speech

Madam Patricia ADUSEI-POKU
Executive Director -
Data Protection Commission

The Executive Director of the Data Protection Commission, Madam Patricia Adusei-Poku in her speech indicated that the Data Protection Commission relaunched to set standards to align it with international best practices in ensuring Transparency, Trust and Transformation. The relaunch also allowed for necessary institutional change to fully establish the need for data protection in Ghana. Noting that transparency provides visibility, ensures fairness in the use of data and reassured the public of the DPC efforts in ensuring that organisations adhere to the laws. She acknowledged the support of certain key industry players, the board of directors, the heads of some institutions and the staff of the Data Protection Commission for their dedication and hard work.

Madam Adusei-Poku reiterated that the new registration software will be beneficial to the Commission and all data controllers, adding that about 200 Data Protection Officers have been trained. Indicating that some institutions now require proof of data protection in organisations before they work with them. There was a video display of the achievements of the Commission so far. She mentioned that the Commission has five new departments which were part of efforts to serve the country better and deliver the DPC's mandate efficiently. The Executive Director outlined the need to be in good standing with the commission as that shows leadership, excellence, builds trust and provides a better business overview. A Memorandum of Understanding (MoU) was signed between the Head of Internal Audit Service and the Commission with regard to training on data protection for staff of the Service.

Keynote Speech

Mrs. Ursula OWUSU-EKUFUL
Hon. Minister for Communications

Hon. Ursula Owusu-Ekuful stated in her keynote speech that Ghana has adopted the ICT for development backed by the ICT4D and that it was important to safeguard data. She mentioned Ghana's effort in Data Protection and acknowledged Ghana's ratification of the Malabo Convention as a bold step, indicating that Ghana is one of the first African countries to have a Data Protection Commission. She mentioned that Ghana organised the first African Data Protection and Privacy Conference which was successful. The Hon. Minister also indicated that the United States Government was also understudying ethics and the Artificial Intelligence of data gathered in Ghana. She also announced that plans are underway to harmonise Data Protection Laws in Africa, adding that there will be



Data Protection Training for approximately 2000 internal auditors. Mrs. Owusu-Ekuful also highlighted some of the challenges faced by the Commission and admonished all to register and pay the necessary fees to enhance the revenue generation of the Commission to aid in its work. She then launched the new registration software and granted 6 months amnesty to all data controllers who have not fulfilled their obligations (regulatory and financial) to the Commission

Awards Ceremony

Some institutions were awarded for their exceptional contribution to the Data Protection Commission and the good work they were doing with regard to data protection in the country. The institutions were; the Bank of Ghana (BoG), National Communications Authority (NCA), Ghana Investment Fund for Electronic Communications (GIFEC), Ghana Gas and the Social Security and National Insurance Trust (SSINT).



SESSION 2

Video Display of the Functionality of the Data Protection Software

There was a display of the functionalities of the new Data Protection software. Some of these were;

- ➔ Arrears generation for data controllers
- ➔ View of data controllers in good standing with the commission
- ➔ Allows upload of pictures and videos
- ➔ Allows payment of fees

About 600 participants took part in the event via the Data Protection Commission's Facebook Page with 200 physical participants



WEEK TWO

BUSINESS FOCAL AREA



CYBERSECURITY
IN THE ERA OF
COVID-19



NATIONAL
CYBER SECURITY
AWARENESS MONTH

WORKSHOP ON IMPACT OF COVID-19 ON GHANA'S DIGITALISATION AGENDA

As part of the National Cyber Security Awareness Month (NCSAM) 2020, the National Cyber Security Centre hosted a Cybersecurity Roundtable Forum on the Impact of COVID-19 on Ghana's Digitalisation Agenda, to discuss the socio-economic impact of COVID-19 on Ghana's digitalisation efforts whilst proffering cyber-resilient measures to secure national digital infrastructure. The cybersecurity roundtable forum also sought to identify the major gaps undermining digitalisation efforts, especially during this pandemic era, to build the trust and confidence of citizens in utilising digital services. In attendance was the Deputy Minister for Communications, Hon. George Nenyi Andah, the Acting Director-General of the National Information Technology Agency (NITA), Mr. Richard Okyere-Fosu, the Managing Director of Cal Bank Limited, Mr. Philip Owiredu, the Director of Health Promotion of the Ghana Health Service, Dr. Da-Costa Aboagye, dignitaries and stakeholders from government institutions and civil society organisations.



Welcome Remarks

Dr. Albert ANTWI-BOASIAKO
National Cybersecurity Advisor

The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako, formally welcomed the dignitaries and all organisations present, highlighting the purpose of the Cybersecurity Roundtable Forum. Dr. Antwi-Boasiako expressed his appreciation to the Government of Ghana and the Minister for Communications for their immense effort in ensuring a safer cyberspace. He further urged businesses to help support a safer cyberspace. Adding that as part of activities and initiatives to secure Ghana's digital ecosystem, the Ministry of Communications launched a Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) in October 2019, which provides platforms and channels for reporting cybersecurity/cybercrime incidents for collation, analysis

and response. Dr. Antwi-Boasiako finally entreated everyone present to report cybercrime/cybersecurity-related issues to the shortcode 292 for necessary actions to be taken.

Welcome Remarks

Hon. George Nenyi ANDAH
Deputy Minister for Communications



The Deputy Minister for Communications, Hon. George Nenyi Andah, in his remarks,

welcomed all to the event, adding that it was aimed at engaging various stakeholders to evaluate the impact of the COVID-19 pandemic on Ghana's Digitalisation Agenda. He further extended greetings from the Minister of Communications, Hon. Ursula Owusu- Ekuful and the Vice President of Ghana and expressed gratitude for their continued demonstration of great leadership and commitment in securing Ghana's Digital Journey. Hon. Andah applauded the President of Ghana, His Excellency Nana Addo Dankwah Akufo-Addo for embracing change and creating a cyber-safe economy. The COVID-19 pandemic has caused numerous changes in the socio-economic life of nations and has challenged the resilience of our cyber system globally.

Digitalisation has proven to be the best practice for businesses and education in this pandemic era, he added. He stated that since March 2020, the NCSC has recorded a significant increase in the number of cybercrime/cybersecurity incidents reported by the public. The government, in collaboration with key stakeholders, need to continually strengthen existing laws to ensure intensified resilience of various ICT systems used by the public and institutions of various sectors in our economy. Adding that, in order to rectify these cybercrime/cybersecurity issues, the Ministry of Communications, through the National Cyber Security Centre has presented the cybersecurity bill before parliament for consideration and enactment by parliament.

Keynote Speech

Mr. Philip OWIREDU

Managing Director Cal Bank Limited



The Managing Director of Cal Bank Limited, Mr. Philip Owiredu, stated that the effect of the pandemic has put much pressure on the financial sector. He further emphasised the need to secure our cyberspace. Mr. Owiredu reiterated that the financial sector is happy about government's efforts in securing cyberspace.

PRESENTATIONS



Presentation

Mr. Richard OKYERE-FOSU
Director-General, (NITA)

The Acting Director-General for National Information Technology Agency (NITA), Mr. Richard Okyere-Fosu, outlined two major initiatives that NITA has undertaken to ensure secure cyberspace in this era of COVID-19 which includes the use of SmartWorkplace office software and Learning Management Systems (LMS). Mr. Okyere-Fosu emphasised that NITA has put together a comprehensive solution to enable all Public Sector workers (MDAs and MMDAs) to stay at home and work remotely while observing all the safety protocols and participating in the government's digital transformation agenda.

Effectively, NITA worked with eSolutions, developers of SmartWorkplace as a virtual workspace solution in response to COVID-19 and as part of the Government of Ghana's digital transformation agenda. Currently,

NITA has successfully deployed the SmartWorkplace solution to 330 MDAs and MMDAs.

This enables public sector workers to work remotely to reduce personal contact, curb the spread of COVID-19 and ensure the safety of public servants. Many government agencies including Cabinet, Ghana Revenue Authority (GRA), Ghana Health Service (GHS), Ghana Standards Authority (GSA), National Pensions Regulatory Authority (NPRA), State Interests and Governance Authority (SIGA), Security and Exchange Commission (SEC) and many more have been trained in the use of the SmartWorkplace office software.

Mr. Okyere-Fosu further elaborated on the Learning Management Systems (LMS) as a response to COVID-19, adding that President H.E. Nana Addo Dankwa Akufo-Addo has given approval for NITA to deploy a Cloud-based Learning Management System (LMS) to facilitate teaching and learning in public universities across the country.

This is a joint project between the Ministries of Communications and Education. He added that NITA will implement the solution with its Technical Partner, Smart Infracore Limited. NITA will also work with GARNET to leverage the GARNET network to the universities, he concluded.

Presentation

Mr. Abraham ASANTE

Administrator, Ghana Investment Fund for Electronic Communications (GIFEC)

In a pre-recorded address, Mr. Abraham Asante, the Administrator of the Ghana Investment Fund and Electronic Communications (GIFEC) stated that one major achievement of the Ghana Investment Fund for Electronic Communications (GIFEC) was in securing the digital space, connecting over 500 remote communities during the COVID-19. This included ensuring all communities were safely connected to enhance easy access to the internet. Mr. Asante, the Senior Manager, Research Monitoring and Evaluation at GIFEC who was present at the event went on to thank the Ministry of Communications for their immense support towards combating the COVID-19 pandemic.



Presentation

Dr. Da-Costa ABOAGYE

Director of Health Promotion –
Ghana Health Service



The Director, Health Promotion, Ghana Health Service, Dr. Da-Costa Aboagye, commended the Government of Ghana for the immense contributions and measures put in place to protect citizens physically and in cyberspace. Many strategies have been adopted to combat the COVID – 19 pandemic, he indicated. These include detection and containment of cases, care for the sick, minimising the impact on economic and social life among others.

achievement of the ADC which included a higher occupancy rate, the number of technology companies hosted at the Centre, partnerships as well as collaborations have increased. Mr. Ofori reiterated that COVID-19 has highlighted the need for a dedicated fund to sustain Ghana's digitalisation agenda. The Digital Innovation Fund will unlock more investment capital for technology-based SMEs in Ghana. This will be a catalytic fund that will do initial investments ranging from Proof of Concept grants to seed investment in convertible debts and other instruments. This fund will serve that purpose so that Tech Entrepreneurs wouldn't have to compete with other businesses for funds.

2.7 thousand people participated via Citi FM's Facebook page with about 150 people present at the venue.



Presentation

Mr. David OFORI

Head of Operations -
Accra Digital Centre

Mr. Ofori stated that the mandate of Accra Digital Centre is to create a conducive ecosystem for digital innovation and entrepreneurship in Ghana. He further outlined the

Closing Remarks

Mr. Frederich Kwakye-Mafo, the lead for CNII at the National Cyber Security Centre, in his closing remarks thanked all present and entreated all to ensure their digital safety. He concluded by adding that although much work had been done, much more needed to be

CYBERSECURITY WORKSHOP ON MOBILE MONEY FRAUD



Welcome Address

Dr. Albert ANTWI-BOASIAKO
National Cybersecurity Advisor

Dr. Albert Antwi-Boasiako in his welcome address noted that mobile money remains one of the most important developmental initiatives, especially with respect to financial inclusion. He noted however that there are specific issues with fraud that have affected the mobile money platform that needs to be addressed. He revealed that data received by the National Computer Emergency Response Team (CERT-GH) of the NCSC indicates that about 50% of fraud cases received are mobile money-related. He stated that mobile money is not one of the highly sophisticated cybercrimes that are known, stressing that 75% of this type of fraud can be prevented if subscribers/users are sensitised

and educated on transaction safety and the various schemes of cybercriminals.

He emphasised the need to engage all stakeholders, especially the public, to contribute in discussions to ensure the prevention and mitigation of mobile money-related fraud.

Remarks

Mr. Derrick LARYEA
Head of Research and
Communications, Ghana Chamber
of Telecommunications

Mr. Laryea noted that Mobile Money is of key importance to the telecommunications industry and couldn't have been discussed at a better time. He further revealed that the Ghana Chamber of Telecommunications has witnessed a spike and increase in the usage

of mobile financial services and digital platforms. He cited an attack on Uganda's Mobile Money platform in recent weeks which caused the suspension of mobile money services in the country for days. He asserted that the mobile money fraud can be categorised and tackled from three (3) angles, namely the People/Users, the Technology component and the Process.



He stressed that Mobile Network Operators (MNO) are ensuring the safety of consumers by putting in place the necessary policies, procedures and technical measures to deter cybercriminals. He reiterated that regulation alone cannot deal with the issue of fraud but collaboration between parties is key to curb the menace. He however stressed that consumers have a significant role/responsibility to play in the fight against mobile money fraud and urged Service Providers/ Regulators to streamline processes in providing respite for consumers. He stressed the need to intensify awareness creation and build capacity among all stakeholders.

Remarks

Mr. Philip Danquah DEBRAH

Head of Business Operations,
e-Crime Bureau

Mr. Debrah highlighted various services and initiatives the e-Crime Bureau has been engaged with including threat and cybercrime intelligence as well as partnering with MTN since 2015 to identify various schemes of mobile money fraudsters and build capacity to mitigate them.

He shed light on a survey on mobile money fraud that is being conducted by the e-Crime Bureau purposely to get input from consumers

on their experiences with mobile money fraud. He revealed that inputs received indicate that 7 out of 10 responders have had an encounter with mobile fraudsters. He further disclosed that a report on the survey will be published in the coming weeks.



Mr. Debrah gave a presentation on the cyber landscape, the various risks, threats and vulnerabilities facing organisations and individuals. He highlighted several services the e-Crime Bureau offers including threat intelligence services, capacity building programmes and certification courses.

PANEL DISCUSSION

Mobile Money Fraud and the Way Forward



The discussion was moderated by Madam Edith Mould, a Senior Consultant with Deloitte. The panel was constituted by;

- ➔ **ACP Dr. Herbert Gustav Yankson** - Director, Cybercrime Unit: Criminal Investigations Department
- ➔ **Mr. Eric Mensah** - Head, Technical Operations, e-Crime Bureau
- ➔ **Mr. Kwame Oppong** - Head of FinTech and Innovation; Bank of Ghana
- ➔ **Mr. Godwin Tamakloe** - Senior Manager - AML, Compliance & Analytics; MTN Ghana

Remarks

Moderator

Madam Edith MOULD

Senior Consultant with Deloitte

Madam Mould in her introductory remarks noted that mobile financial services have become a rapid area of development within the African emerging markets. She revealed that there is a minimum of 866 million transactions globally on a daily basis with as much as 4 billion dollars in value of transactions. She stated that the main motive of cyber fraudsters is financial gain and with this volume and value of transactions, there is a need to discuss the modus operandi and schemes through which these fraudsters are able to successfully defraud their victims. Madam Mould posed various questions to the panelists and gave participants the

opportunity to contribute and ask related questions.

Mr. Godwin TAMAKLOE

Senior Manager – Compliance and Analytics, MTN Ghana



Mr. Tamakloe in his opening statement noted that the issue of fraud has persisted within the

financial sector, across the world for which mobile financial services is no exception. Addressing the various trends that fraudsters have adopted, Mr. Tamakloe noted that smishing and vishing have been the most used techniques coupled with emotional stories to socially engineer victims into sending money.

Loss of trust, reputational damage and decreased revenue, he stated, are some of the risks mobile network operators face with respect to mobile money fraud. He posited that mobile money fraud can only be mitigated if stakeholders work together as a collective body. Mr. Godwin Tamakloe entreated all stakeholders including regulators to join forces in creating the necessary awareness on mobile fraud to all consumers, especially in various regions and organisations including schools and community centres. He revealed that over 50 arrests have been made in collaboration with law enforcement and MTN is committing about \$2.5million to secure a platform with machine learning and artificial intelligence features to enhance monitoring and security of the MTN mobile money platform. He encouraged users to have confidence in using the platform. Mr. Tamakloe shared several tips and advisories on how to prevent mobile money fraud.

Mr. Eric MENSAH
Head of Technical Operations,
e-Crime Bureau

Mr. Mensah highlighted various vulnerabilities that mobile money fraudsters exploit to commit fraud.

The lack of security consciousness, he stated, is the most preyed on vulnerability by cyber fraudsters. He further mentioned that most consumers of mobile money are ignorant of the various schemes of mobile money fraudsters. Mr. Mensah emphasized that the improper registration of SIM cards is a major factor in solving mobile money fraud because it is the link to properly identify fraudsters for apprehension and prosecution.



To prevent the prevalence of mobile money fraud, Mr. Mensah stressed that there is a need to intensify awareness creation and control of access rights on the side of service providers. Effective monitoring, he stated will go a long way in the detection of fraudulent transactions. He added that policies need to be developed to control and monitor the activities of third-party systems which interface with the mobile money platform. Mr. Mensah stressed that there is a need to enforce existing regulations and encourage participants to ensure due diligence in mobile money transactions.

ACP Dr. Herbert Gustav YANKSON
Director Cybercrime Unit,
Ghana Police CID

ACP Dr. Yankson revealed that mobile money platforms have become the preferred mode for cyber fraudsters mainly because it connects to almost all facets of the financial sector. He also mentioned that mobile money platforms are also preferred for illicit financial flows. He further revealed that the Criminal Investigations Department has witnessed an increase in the number of mobile money fraud cases being reported, disclosing that a total of about \$ 93,000,000 was lost to fraud in 2018 alone, the figure however decreased significantly in 2019. He stated that as of June 2020, the CID headquarters alone has recorded a total of about \$ 49,000,000 lost to cyber fraudsters. Dr. Gustav Yankson stated that mobile money fraudsters have moved from social engineering



as a scheme of defrauding to more sophisticated means through the use of technology (spoofing). He re-echoed that there is a need to intensify awareness creation and

capacity building among all stakeholders, to effectively mitigate mobile money fraud. ACP Dr. Yankson stated that service providers need to adopt the Know Your Customer (KYC) guideline to validate identity cards presented for registration of SIM cards and services, this he said will help in the easy identification of cyber fraudsters. ACP Dr. Yankson, in concluding, entreated all stakeholders to collaborate with law enforcement agencies in mitigating cyber fraud.

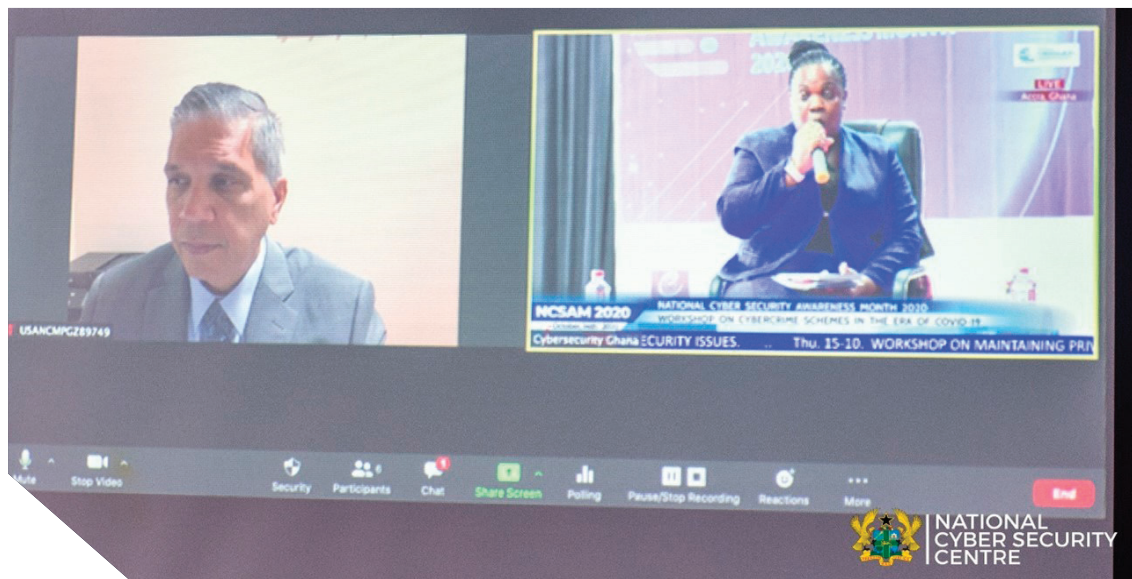
Mr. Kwame OPPONG
Head of FinTech and Innovation,
Bank of Ghana

Mr. Oppong, in his submission, emphasised that the issue of mobile money fraud affects both consumers and service providers. He opined that the menace can be best tackled/mitigated when a multi-stakeholder approach is adopted. Mr. Oppong highlighted that one of the actions the Bank of Ghana took was to update the law on payments to go beyond the Electronic Money Issuing Guidelines (EMI) which was published in 2015 to a Payment Systems and Services Act which identifies, regularises, licenses and supervises FinTechs and third-party applications that integrate with payment systems. He stated that any form of financial service is based on trust.



It is therefore the responsibility of financial service providers to ensure adherence to standards and regulations. He reemphasised that the challenges in mitigating mobile money fraud can also be attributed to the weak identity system of the nation and reiterated that the introduction of the National Identification System is a step in the right direction that will go a long way to address most of the issues. Mr. Oppong in his closing remarks encouraged all stakeholders to report the issues and irregularities they face to authorities as it will inform the policy direction of the Central Bank. The workshop was widely received with over 1.3 thousand views via Facebook and about 250 people participating physically.

WORKSHOP ON CYBERCRIME SCHEMES IN THE ERA OF COVID-19



The COVID-19 pandemic is having a dramatic impact on society and has forced everyone to become heavily reliant on the internet and its digital economy. This has increased the attack surface exponentially and multiple vectors for cyberattacks through the heightened dependency on digital services. According to one of INTERPOL's private sector partners, 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs — all related to COVID-19 were detected during the first four months of 2020. The financial impact of cybercrime is rising each year and losses for 2020 is expected to exceed the \$9.8 million loss recorded for 2019 by the Criminal Investigations Department (CID). The National Cyber Security Centre, through its cybercrime/cybersecurity incident reporting points of contact (POC), has received over 11,500 reports since the pandemic was announced.

The crimes fluctuate from ordering high demand products (i.e., masks and hand sanitisers) which never arrive, Mobile Money scams, economic relief programs, fake news, impersonation of organisations and government officials.

To address the need to create awareness and build resilience, the National Cyber Security Centre hosted a workshop aimed at creating a platform for the discussion of popular Cybercrime Schemes prevalent in the Era of COVID-19 and propose possible mitigation strategies for the benefit of the four pillars of the A safer Digital Ghana awareness campaign (Children, the Public, Business, and Government).

The meeting was attended by officials of the National Cyber Security Centre, officials of the National Security Council Secretariat, officials of the Financial Intelligence Centre,

officials of the US Department of Justice and officials of ISC2.

Welcome Address Dr. Albert ANTWI-BOASIAKO National Cybersecurity Advisor

In his remarks, the National Cyber Security Advisor stated that Ghana has recorded several COVID-19 related cybercrimes. He noted



that the health sector was one area heavily impacted by COVID-19 schemes because, criminal groups all over have targeted it, seeking to undermine the health sector infrastructure worldwide. Malicious campaigns targeting people, fake news and malware programs were distributed with COVID-19 emails. Generally, there have been malicious campaigns and misinformation about medication available for COVID-19 related diseases. He further stated that as a community, we need to come together to discuss how this disease is affecting us, the goal being to seek the safety of all stakeholders. He invited participants to cover and share experiences to help build a better picture of the situation in order to fight cybercrime effectively.

Message from Sponsor Deloitte Ghana

Deloitte.

Deloitte Ghana highlighted the high-quality services they provide for an ever-changing threat landscape. The details of those services include advisory and cybersecurity implementation services and advanced managed security services through a mature global network of advanced security operations. These include threat intelligence, threat gathering and security analytics. Additional offerings such as application security testing and cyber incidence response are also

available depending on the needs, size and maturity of the organisation in question. Deloitte also indicated that they tailor solutions to meet the most critical business needs. The sponsor urged listeners to think of Deloitte whenever they think about cybersecurity.

Presentation

Mr. Kofi BOAKYE
Financial Intelligence Centre



In his presentation, Mr. Kofi Boakye of the Financial Intelligence Centre introduced the audience to the purpose and mandate of the Financial Intelligence Centre (FIC) through a video presentation. The video outlined various transactional scenarios in which the FIC is required to be alerted and a process flow of how the FIC coordinates with other law enforcement, security and government agencies. He stated additionally that the FIC was established in accordance with section 4 of the Anti-Money Laundering Act, 2008 (Act 749).

He added that the FIC receives different types of reports from the general public and as well indicated that the FIC receives financial disclosures of the following types: Suspicious transaction reports, Cash Threshold reports, Electronic funds transfer reports above the threshold, Full Account Disclosure reports on request from the bank, politically exposed person reports and Terrorist financing reports. He further outlined observations that have been made by the FIC based on analysis of the data they have collected over a period. He mentioned how the FIC is fighting Money Laundry and stated that Ghana is currently on a grey list of the Financial Action Task Force (FATF) because of the prevalence of online fraud, fake COVID-19 materials offered for sale and the sale of huge amounts of medicines outside authorised networks which required the transfer of huge sums of money as payment. He mentioned ATM fraud as an example of newer ways criminals tend to beat showcased cases through a short video documentary. In this video, several passengers were stopped by customs and immigration officers for carrying several ATM cards that were not registered in their name. One such case was of a man carrying 2,830 valid ATM cards concealed in a box of noodles. This was a way of moving large amounts of money without triggering the attention of Nigerian authorities. He concluded with a series of admonishment highlighting the way forward and asked the audience to form individual opinions based on all that they had heard.

Message from Sponsor

Technosol Limited- THALES

In a short message by the sponsor, THALES stated that the people the world relies on for progress depend on THALES to make life better and keep us safer. Combining a unique mixture of expertise, talents and cultures, THALES architects design and provide extraordinarily high technology solutions to make tomorrow's technology possible today across the world and in cyberspace. THALES helps their customers think smarter and act faster, mastering every great diversity and decisive moment along the way. The message ended with the THALES logo which also featured its slogan- Together Safer Everywhere.

PANEL DISCUSSION

The panel discussion was done by experts from various institutions across the CERT-GH ecosystem. These include officials of the National Cyber Security Centre (NCSC), officials of the National Security Council Secretariat, officials of the Financial Intelligence Centre, officials of the US Department of Justice and officials of ISC2. The session was moderated by Mr. Osei Bonsu Dickson, a Chief Legal Advisor at the National Security Council Secretariat and the team of panelists constituted Mrs. Audrey Mnisi Mireku, the CERT Lead of the



NCSC, Mr. Anand Ramaswamy, an assistant US attorney and Mr. Eric Amoah Damson, an information security data analytics and privacy professional.

Discussion Prevalent Cybercrime Schemes in Ghana

The moderator began by introducing the panelists and restating the topic for discussion. He asked Madam Mireku to acquaint the audience with the prevalent cybercrimes in Ghana. After her remarks where she lists cyberbullying, online child abuse, web defacement, impersonation amongst others, the moderator Mr. Dickson gave his take on the same question, where he highlighted phishing as another popular cybercrime being employed by criminals to attack unsuspecting people. The moderator further asks Mr. Damson to expand on the mentioned phishing schemes. In response, he used a few scenarios to explain the modus operandi of the phishing attack. Mr. Dickson also asked Mr. Ramaswamy to throw light

on the same issue from an American perspective. Here, Mr. Ramaswamy stated COVID-19 themed phishing and BEC attacks, websites that sell medicines and fake cures for COVID-19 and identity theft to access multiple relief packages and funds from governments.

Discussion Common Cybercrime Schemes at Regional Level

The moderator began another discussion bordering on cybercrime schemes that are prevalent at the sub-regional or regional level in Africa. Madam Mireku stated that intelligence for cybercrime at the regional level is very similar to cybercrimes in Ghana. She stated that cybercrimes at the regional level are repeated but customised for the Ghanaian region. The moderator asked Mr. Damson if he can add to this observation. Mr. Damson indicated that fear and panic enable cybercrime.



Madam Mireku also added to her earlier submission, by stating that Recruitment Fraud has also become the order of the day, where cybercriminals pose as politically influential Personnel and dupe people through fake job offers, opportunities and business transactions. She mentioned the cloning of business websites by criminals who replace legitimate contact addresses with fake contact addresses. The moderator requested statistics of cybercrime in Ghana.

In response, Madam Mireku mentioned that from January to August about 11,545 incidents had been recorded by NCSC, of which 50% constituted online fraud, 15% were the publication of non- consensual intimate images, 9% online impersonation and the rest being disinformation, misinformation and advisories for concerned parents seeking online safety of their children.

Discussion

Relevance of Legal Provisions for Cybercrime

The moderator then asked about benefits derived from the Malabo Convention. To which Mr. Ramaswamy stated that the main

advantage of the treaty is the harmonisation of law among member states and that is key to the successful prosecution of many cybercrimes that cut across borders. The moderator then asked Madam Mireku if there has been any follow up after Ghana acceded to the Budapest Convention last year. Madam Mireku stated that the Ministry for Communications has organised workshops for judges, sensitisation workshops nationwide, and training for the Mobile Network operators to aid cybercrime prosecution. The moderator asked Mr. Damson what the effect of ratification of international conventions have been on the private sector. Mr. Damson stated that these laws and policies direct the private sector as to which direction to go in terms of cybersecurity development such as how to keep and protect customer data. The moderator asked Mr. Ramaswamy to explain why cybercrime is still rising if effective measures (prosecutor laws) have been established. Mr. Ramaswamy indicated that ensuring cybersecurity is an ongoing process where cybercriminals try to outsmart law enforcement agencies in preventing current and future criminal activities. The moderator asked Madam Mireku to describe the kinds of ongoing investigations in Ghana and how we can delve into their effectiveness. It was indicated that cultural issues like a lack of confidence to report, gaps in terms



of skills, technology, professionals and law enforcement were some of the challenges faced. She added that there was a need for more collaboration between the government and the public to fight cybercrime. In conclusion, the moderator asked Mr. Damson to highlight some of the issues with cybersecurity education in contemporary times. To which he noted there is a notable gap in Ghana's educational system where there is no element of security in the ICT curriculum, which results in a vulnerable future generation being susceptible to common cybercrimes like mobile money fraud and so on.

At this point in the session, there were interactions between the audience and panelists on what can be done further to mitigate cybercrime schemes, the present measures that have been put in place and what people need to know about the government's cybersecurity development. Questions were asked from the audience regarding cybersecurity policy direction, initiatives to create cyber awareness within educational institutions, how the government is mitigating cybercrime related to digital currencies, government initiatives to change the psychological mindset of potential and practising criminals, improvements in the procedures to handle cybercrime, and opportunities in cybersecurity.

Closing Remarks

Participants were encouraged to utilise the various channels of the Cybercrime/Cybersecurity Incident Reporting Points of Contact to report cybercrime and cybersecurity issues for assistance, guidance and remediation. 200 participants were present at the venue with about 600 online participants.

WORKSHOP ON MAINTAINING PRIVACY ONLINE IN THE ERA OF COVID-19



Dr. Albert ANTWI-BOASIAKO National Cybersecurity Advisor

As the coronavirus pandemic takes its toll on human life and livelihoods, governments, public-health authorities, companies, and individuals have responded with extraordinary measures. To protect the health of people, governments and institutions put in place restrictions on movement and mechanisms for health tracking and reporting. These mechanisms, including contact-tracing and self-reporting apps with some recording and transmitting personal health information, underscore the deepening importance of data protection and privacy in this crisis. The pandemic has led to rapid digital transformation nationally which is of great importance to improve the functioning and efficiency of public and private organisations,

as well as the well-being of populations. The outbreak has led to a shift in consumer behaviour with individuals upgrading their broadband speeds and participating in more online activities. As the value of digital infrastructure increases, connectivity will be seen as a human right.

In this pandemic, understanding and managing the inherent risks associated with working remotely will allow organisations to better understand priorities and controls to put in place in order to protect data.

The workshop equipped participants with the needed information to protect data as they access online platforms. The event engaged representatives from Heads of Security Agencies, Members of the National Cyber

Security Technical Working Group (NCSTWG), agencies of the Ministry of Communications, Government Institutions, Telecommunication Institutions, Academic Institutions, Private Sector CEOs, Civil Society Organisations and Religious Groups. The workshop began with a pre-recorded welcome address by the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako. He mentioned the importance of data protection and citizens' rights to privacy. He also discussed issues relating to the enforcement of citizens' rights to privacy.

Opening Remarks

Valerie Hudson

Deputy Executive Director,
Data Protection Commission

Madam Valerie Hudson, the Deputy Executive Director of the Data Protection Commission (DPC) then gave the opening remarks. She talked about the growing use of digital services resulting from COVID-19 and then mentioned how privacy safeguards can be ensured in the era of COVID-19. Madam Hudson then went ahead to talk about how institutions are expected to comply with Data Protection regulations especially in the era of COVID-19.



Presentation The Obligations of Data Controllers and Processors

A presentation on Obligations of Data Controllers and Processors by Mr. Seth Fosu-Kwarteng, the Human Resource Manager of DPC followed. The objective of the presentation was to give an overview of the DPC,



its mandate, Data Controllers and Processors and their obligations under the Data Protection Act. He stated that the mandate of DPC is to protect the privacy of individuals and personal data.

He mentioned some key terms to data protection to include; personal data, data subject, data controller (Any institution that determines the purpose and means of processing data), data processor (Any institution who processes personal data on the instruction of a data controller), processing and consent. Mr. Fosu-Kwarteng then took the participants through some of the principles of data protection according to section 17 of the Data Protection Act, 2012 (Act 834) on standards that guide data controllers and subjects on data protection. The following principles were enumerated; accountability, openness, the lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, quality of information, data subject participation, and data security safeguards. He concluded by stating the key obligations of data controllers which is to implement appropriate technical and organisational measures.

Presentation Data Protection Software

Mr. Dennis Darkwah, the Head of Regulations and Compliance at the DPC then gave a presentation on the newly launched Data Protection Software. The objective of his presentation was to demonstrate steps to registration using the DPC registration software. He started by stating that 'Compliance of Data Protection is a journey' and that one of the key functions of the Commission is to keep and maintain a Data Protection Registry hence the need for the application.

He then demonstrated the DPC website and registration software. The DPC Website can be accessed at <https://www.dataprotection.org.gh/register>. He mentioned that the platform helps to search for entities in good standing with the Data Protection Commission by checking the statuses of their registration. Key features of the system include; Payment & Invoices, Roadmap and Risk Assessment Questionnaire,



Uploading Evidence/Documents and Managing Online Accounts & Payments. The registration steps also include; Registration Process, Questionnaire, Details, Capacity, Processing, Contacts, and Documents Invoices. He further added that the cost implications of registration for small scale organisations is GHs 120.00, for medium scale organisations is GHs 900.00, and for large scale organisations is GHs 1,800.00. He added that per the Data Protection Act, every organisation is mandated to register regardless of whether sector awareness is done to all controllers and data subjects. He also stated that according to section 95 of the Data Protection Act, 2012 (Act 834) non-compliance and defaulters may be liable to a prison sentence and 5,000 penalty points. He ended by stating that DPC does not manage data but rather regulates institutions to ensure data protection compliance.

Presentation Complying with the Provisions of the Data Protection Act, 2012 (Act 834)

A presentation on “Complying with the Provisions of the Data Protection Act” by Dr. Patrick Adonoo, Director of Regulations and Compliance at the DPC followed. The purpose of his presentation was to inform data subjects of their rights and the importance of data protection compliance for data controllers and processors.

He stated that the wealth of institutions in the modern world can be measured by the volume of data they collect. ‘Data is the new gold’, he said. He identified the key relationships of DPC comprising of the following; data controller, data processor, data subjects (Individuals), third parties and third countries. He added that the DPC teaches data subjects the rights to privacy that they have. He added that the issue of data protection is very critical hence the need to demand accountability from data controllers. He stated also that the DPC teach data controllers their duties and roles to ensure data protection compliance. On the issue of third country data transfers, the DPC has the following in place; rights of a data subject, right to be informed, right to give and withdraw consent, right of access to personal information, right to amend (rectification), right to object, right to complain and the right to compensation. He mentioned some of the benefits of complying with the Data Protection Act to include the following; demonstrating an accountable and responsible organisation, gaining customer trust and confidence, data protection compliance is recognised as a business differentiation factor globally and enables a clearer understanding and business overview for key decision-makers (Board members). He concluded on the role of data protection supervisors (Section 58) appointed by institutions to ensure data protection compliance which is to monitor compliance.

Presentation The Effect of COVID-19 on Privacy and Data Protection

A panel discussion that commenced after the health break followed. The panelists were Mr. Isaac Socrates Mensah of the National Cyber Security Centre (NCSC), Mrs. Sylvia Gifty Appiah of Information Governance Solutions, Mr. Ludwig Marcus Schandorf of Ghana Export Promotions Authority (GEPA), Dr. Kwabena Owusu Danquah of the Kwame Nkrumah University of Science and Technology (KNUST) and Mr. Dylan Kwablah Kewlett of Social Security and National Insurance Trust (SSNIT) as the moderator for this session. The theme for the panel discussion was “The Effect of COVID-19 on Privacy and Data Protection across Institutions in Ghana”.

The session began with introductory remarks by Mr. Mensah on the need to look at the security aspect of digitisation in the era of COVID-19. He highlighted the need to look at technical measures and how well



individuals are securing their private information online.



Madam Sylvia Gifty Appiah then gave her opening remarks, stating that data protection is a fundamental human right, adding that personal information is the fuel that runs businesses. Employees are also data subjects and organisations have an obligation to protect employee data.

Mr. Ludwig Marcus Schandorf, when asked how to ensure compliance with data protection when working remotely, responded stating that it is safer to work from the workplace



than remotely due to the higher risks of exposing personal data when at home. He mentioned that Ghana Export Promotion Authority (GEPA) performed a risk assessment before migrating to virtual conferencing when the pandemic started. They realised Microsoft Teams was one of the most secure software to use for their organisation.

Dr. Danquah then mentioned that the DPC has a lot of work to do when it comes to the health sector and hospitals in Ghana because the risk of having a software hack and sensitive data being exposed is high. A participant asked the panelists if there are any indicators to check before using a video-conferencing application. To which he was told that there are functionalities in the settings of an application that enable unique accesses and so users can utilise them.

The panelists were then asked ways by which individuals can take charge to protect their personal data. To which the panelists answered that individuals should ensure that they insist on their rights as data subjects and ensure data controllers comply with the Data Protection Act 2012 (Act 834). The audience were also advised to ensure due diligence when they go online to use websites and try as much as possible to report incidents to the National Cyber Security Centre and the Data Protection Commission. Panelists were also asked how to resolve devices with malware that can steal data on a computer.

To this, they advised that individuals should use corporate devices when working from home because of the



security controls installed on them. The panelists added that personal devices are threats to corporate servers, unlike corporate devices.

Finally, the panelists were asked what happens after COVID-19 and what happens to our data looking forward. They answered that in terms of utilisation of conferencing technology, it is going to continue to grow, hence steps have to be taken to continue to protect our data. Additionally, data relative to COVID-19 should be handed over to the Ministry of Health to plan for the emergence of a similar magnitude. They advised that as much as possible, data should be anonymised to include just the statistical data.

To conclude the session, Mr. Raynolds Nyarko Darko thanked everyone for taking time to attend. He also thanked the National Cyber Security Centre and mentioned that the Data Protection Commission will collaborate more in the future.

JOINT FREEDOM ONLINE COALITION (FOC)/ NATIONAL CYBER SECURITY CENTRE (NCSC)

Digital Inclusion In The Era Of COVID-19

As part of the 2020 edition of the National Cyber Security Awareness Month (NCSAM), the National Cyber Security Centre together with the Freedom Online Coalition organised a virtual session on Digital Inclusion in the Era of COVID-19. Following the Governments of Ghana and Germany co-producing and launching a Joint Statement on Digital Inclusion at the 8th Annual Freedom Online Conference in Accra, Ghana, both governments recognised the importance of meaningful digital inclusion in enabling people to exercise their fundamental freedoms fully. The document also acknowledged that persisting discrepancies in access creates digital divides, which often reinforce existing social and economic inequalities, and prevent people from realising their full potential and benefits provided by the Internet.

This session addressed issues such as digital inclusion and unequal access in an increasingly digitised world and, particularly, Africa. It focused on ensuring that ICT does not further reinforce existing inequalities but rather bridge the existing knowledge and socio-economic gaps. The session took place on Thursday, October 15, 2020, and commenced at 9.00am via Zoom. The event brought together representatives from the Freedom Online Coalition Support Unit, the Governments

of Ghana and Germany, including other representatives who have an interest in digital inclusion.



Opening Remarks

Dr. Albert ANTWI-BOASIAKO
National Cybersecurity Advisor

The event began with opening remarks by the National Cybersecurity Advisor, who welcomed all present and expressed his appreciation to the Freedom Online Coalition and the applaudable work they have done with regards to ensuring the freedom of internet users. He went on to speak about how the COVID-19 pandemic has proved the need for ICT and digital inclusion. He further iterated the need for the internet to be made available to underserved and unserved communities so as to

bridge the digital divide and ensure digital inclusion. He acknowledged the Joint Digital Inclusion statement by the Governments of Ghana and Germany and emphasized the need to work with civil society organisations, the private sector and multi-stakeholders to ensure digital inclusion.

Panel Discussion Digital Inclusion and Unequal Access

The session was moderated by Ms. Minna Pentilla from the Freedom Online Coalition and Ms. Emmanuella Darkwah from the National Cyber Security Centre. Ms. Pentilla began by introducing the speakers/panelists for the day who included;

- ➔ **Hon. Sam Nartey George**
Member of Parliament, Ghana
- ➔ **Mr. Victor Asante**
Ghana Investment Fund for Electronic Communications (GIFEC), Ghana
- ➔ **Ms. Swantje Maerker**
Federal Foreign Office, Germany
- ➔ **Mr. Edetan Ojo**
Media Rights Agenda, Nigeria
- ➔ **Ms. Vivian Affoah**
Media Foundation for West Africa, Ghana

Hon. Sam Nartey George thanked the NCSC and the FOC team for organising the meeting and asked that all participants focus on the discussions for the day and make valuable contributions. He went on to speak on internet access and two issues concerning it that need to be critically looked at. He mentioned that there needed to be a focus on dedication to access and funding of the internet. He said that governments needed to put in place policy directives to ensure that all citizens have access to the internet and bridge the digital divide.

Mr. Victor Asante from GIFEC thanked the team for the opportunity and begun by indicating how connectivity to the internet has always been an issue but the Government of Ghana, through the Ghana Investment Fund for Electronic Communications (GIFEC) has been trying to bridge the gap of connectivity to the internet especially in unserved and underserved communities. He mentioned that a survey conducted showed that children in underserved communities were missing out on school activities especially during the COVID-19 pandemic because of lack of access and only 1% of households had access to the internet. He iterated the need to ensure that internet connectivity is extended to the furthest part of unserved and underserved communities.

Ms. Swantje Maerker, the representative from the German Federal Foreign Office, in her opening remarks, thanked the team for the opportunity and touched on the challenges COVID-19 has had on digitalisation.

The Executive Director of Media Rights Agenda in Nigeria, Mr. Edetaen Ojo, spoke about digital inequality and the divide that exists as well as its effects. He mentioned how the lockdown in most countries due to the pandemic exposed the importance of the digital world. He also mentioned how the social, economic, and political livelihoods of citizens have been affected.

Madam Vivian Affoah, the representative from the Media Foundation for West Africa began by speaking on the lack of access and how it affects daily life. She highlighted the significance of meaningful access and communication.

Ms. Swantje Maerker expressed her support for the recommendations from the Digital Inclusion Statement and threw more light on the need for a task force to ensure the implementation of the recommendations indicated in the statement. Madam Vivian Affoah suggested that government can create an enabling environment for CSOs to thrive and contribute to such discussions. She applauded the work of CSOs in ensuring digital inclusion and the freedom and rights of internet users and asked that the interventions by governments to bridge the digitalisation gap be inclusive of multi-stakeholders.

Mr. Edetaen Ojo highlighted the issues surrounding media illiteracy and digital illiteracy as some of the challenges for digital inclusion. He then suggested some efforts that can be put in place to bridge the divide. He reiterated the need for the task force to implement recommendations from the statement and asked the general public to study the statement and identify areas where they will require assistance.

In his remarks concerning the cost of ensuring connectivity and internet access, Hon. Sam George mentioned that governments need to take proactive steps to address

the issue of cost when it comes to digital inclusion. He suggested the reduction of the cost of internet data and the need to invest in high-speed internet at reduced prices.

Final Remarks

Mr. Edetaen Ojo indicated that Governments need to ensure that the citizens have access to the internet and maintain a positive attitude towards achieving digital equality and inclusion. They can then leverage this to invest in internet access. Ms. Swantje Maerker called for multi-stakeholder cooperation and work toward implementing the content and recommendations from the joint digital inclusion statement. Mr. Victor Asante reiterated the need to engage key stakeholders to ensure that the work done will benefit every individual. He added that there is also a need to discuss access as a basic right of the individual.

Hon. Sam George further stressed the need to see access as a right issue. He called on the FOC to ensure that legislation in Africa pushes for the freedom of access to the internet. He asked that country leaders sign a declaration for their citizens to enjoy the right to access.

Closing Remarks

Ms. Minna Penttillä thanked all the participants and panelists and mentioned that Finland will chair the Freedom Online Coalition in 2021 and called for support and cooperation in ensuring the rights of the individual online. Ms. Emmanuella Darkwah concluded the session by thanking all participants present for contributing significantly to a fruitful discussion and thanked the FOC for partnering with the NCSC in organising a very successful event. 70 participants joined the zoom platform for the event.

WEEK THREE

PUBLIC FOCAL AREA



CYBERSECURITY
IN THE ERA OF
COVID-19



NATIONAL
CYBER SECURITY
AWARENESS MONTH

CYBERSECURITY FORUM WITH INDUSTRY PLAYERS



The COVID-19 pandemic has created an enormous challenge for businesses worldwide to continue operating despite massive shutdowns of offices and other facilities with data centres, cloud systems, servers, digital devices and their now-remote employees becoming more vital than ever. The demand placed on the digital infrastructure has skyrocketed overnight with collaboration technologies becoming a very lucrative target for cybercriminals. The COVID-19 pandemic has also led to potential delays in cyber-attack detection and mitigation as evidenced in a number of reported cyber breaches. The activities of many security teams have been impaired due to the pandemic thereby making detection of malicious activities more difficult and complex. Chief Risk Officers (CROs) and Chief Information Security Officers (CISOs) have

become more relevant than ever. Evidently, cybersecurity underpinned by proper risk management procedures, stringent recovery plans, good information security policies and strategies, incident management and response procedures, compliance and monitoring mechanisms and capacity building for staff has become imperative to ensure the business continuity of organisations in this era.

The event engaged representatives from the National Communications Authority, Government Institutions, Banking & Finance, Telecommunications Sector, Audit Firms and Internet Service Providers, among others.

Opening Remarks

Dr. Albert Antwi-Boasiako, the National Cyber Security Advisor began by acknowledging the dignitaries present. He continued by stating that this year has seen a lot of sectors take a deep economic meltdown. The outbreak of the coronavirus pandemic has further caused the dive which has caused a global ripple effect and resulted in closure of borders including air, sea and land as well as physical spaces to ensure the observance of social distancing protocols as part of safety measures to prevent the spread of the pandemic, he said. He continued by noting that individuals have had to make very drastic adjustments to ensure their personal security and that of their respective businesses. Businesses and corporate institutions have had to bear the harsh effects of COVID-19 with some having to lay off their employees.

As a result of the reduction in the existing workforce and higher cost of production, most businesses have had to re-strategise in order to stay afloat. As part of the re-strategising efforts, individuals and businesses have had to migrate their interactions onto digital platforms. The pandemic has necessitated that most people work from home and consequently deploy virtual platforms to facilitate transactions. He mentioned that an assessment by the International Criminal Police

resilient to cyber-attacks and build the capacity of staff in the area of cybersecurity. He also mentioned that it has become a critical factor for organisations to prioritise cybersecurity and ensure the full operationalisation of relevant cybersecurity directives and standards. He said that the discussion will border on the role of private sector stakeholders in Ghana's cybersecurity development, having in view the consequence of COVID-19

as another intervention that seeks to bring the private sector to the government in terms of interactions. He further informed the audience that, the World Economic Forum has approached the Ministry of Communications through the National Cyber Security Centre, to initiate a public-private partnership programme on cybersecurity beginning 2021. This is in view of the strong commitment made by government relative to cybersecurity according to the World Economic Forum. This initiative is expected to strengthen the private and public sector in improving the nation's cybersecurity readiness. He ended by stating that he hoped that the engagement will further highlight the critical issues and the way forward towards the common goal of securing Ghana's digital journey. He also thanked all participants for their participation.



Organisation (INTERPOL), posited that organisations and critical infrastructure have become major targets for cyber-attacks during the pandemic as more people employ the use of ICT. He cautioned businesses and government agencies to be very mindful of the possible cyber threats that could accompany the use of the digital space. Additionally, he mentioned that as corporate entities, the core functions ride on the shoulders of technology infrastructure which mostly are in the hands of private sector stakeholders. In this regard, it is important that organisations improve upon cybersecurity posture to make systems more

on Ghana's digital economy. He also touched on post COVID-19 initiatives that organisations must operationalise to safeguard the digital ecosystem especially for the protection of Ghana's CII. He added that two critical developments have been made by the government to improve cybersecurity development in the private sector. One is the revision of Ghana's National Cybersecurity Policy and Strategy which has placed the private sector, either those who operationalise the platform or even cybersecurity companies and firms, at the centre. The second is the introduction of the Cybersecurity Bill that seeks to regulate the ecosystem and serve



Keynote Speech

Hon. Alexander K. K. Abban

Deputy Minister For Communications

The opening remarks were followed by a keynote speech by Hon. Alexander K. K. Abban, a Deputy Minister of Communications and Member of Parliament for Gomoa West Constituency. He gave the keynote speech on behalf of the Minister for Communications, Hon. Ursula Owusu-Ekuful. The Deputy Minister welcomed and thanked the audience for their continuous participation in the 2020 National Cyber Security Awareness Month (NCSAM). He mentioned that their participation in the month-long event is a demonstration of their commitment to ensuring the development of Ghana's cybersecurity. He added that the platform sought to access the overall impact of COVID-19 on the operations and overall cybersecurity posture of the various organisations. He went ahead to state that, the outbreak of COVID-19 has caused

a paradigm shift across all sectors of the economy and further necessitated a migration onto various digital platforms to ensure effective communication and access to services in order to meet up with necessary growth and productivity. This increased digital citizenship has also heightened the threat landscape in the cyberspace and hence called for increased vigilance among all internet users. The Government of Ghana as the key champion of the country's cybersecurity development and in recognition of the increased digital citizenship over the past few years has put in place a number of priority and strategic initiatives underpinned by the digital Ghana agenda to ensure the cyber resiliency of Ghana's digital ecosystem. He mentioned that the Ministry of Communications (MoC) through the NCSC has implemented key initiatives to

consolidate cybersecurity efforts in Ghana. Paramount among the initiatives is the introduction of a Cybersecurity Bill which is currently pending Cabinet's approval for onward submission to Parliament to be subjected to Parliamentary proceedings before being enacted into law. When passed into law, he said, the Cybersecurity Act will serve as a legal instrument to regulate cybersecurity activities while providing the basis for the establishment of a Cyber Security Authority (CSA) and the protection of Critical Information Infrastructure (CII) among others. The Cybersecurity Bill also has provisions that seek to promote the development of the cybersecurity ecosystem including the private sector by way of research and development, education, standardisation, accreditation and certification of cybersecurity

professionals, products and services.

He mentioned that the Ministry of Communications through the NCSC has also conducted an extensive review of the National Cybersecurity Policy and Strategy (NCPS) to reflect current trends in cybersecurity. He ended on the note that with the advent of COVID-19 and its impact, it has become imperative that we gain additional views of industry players in order to improve collaboration and resilience relative to cybersecurity. He further added that the NCPS is envisaged to serve as a benchmark instrument to provide policy direction and an implementation tool to cybersecurity initiatives.

“As an integral part of cybersecurity development in Ghana, the NCPS is envisaged to provide an operational framework that would promote and encourage the development of industry players and private sector stakeholders”.

As a strategic imperative to develop national capacity, he added that government will actively pursue and develop the local cybersecurity industry by promoting relevant investments and public-private partnerships as the development of the local industry constitutes an important element of Ghana’s goal for cybersecurity resilience. He stated that the Ministry, through the NCSC, has developed a draft Critical Information Infrastructure (CII) Directive that prescribes baseline cybersecurity requirements for all designated CII owners including the health and finance sectors. Additionally shared was that for industry players who operate and control critical infrastructure, the Directive being developed will

ensure that all industry players implement robust cybersecurity mechanisms and frameworks to make systems more resilient to cyber-attacks. He thanked the industry players for their unflinching support in the government’s multi-stakeholder engagement in ensuring a resilient cybersecurity architecture. He implored all industry players to actively engage in this workshop so that solutions can be proffered towards ensuring the security and resilience of the systems in organisations.

Presentation Maintaining Cybersecurity Compliance in the Era of COVID-19



The CEO of Innovare, Mr. C.K. Bruce gave the first presentation on Maintaining Cybersecurity Compliance in the era of COVID-19. He congratulated the NCSC for the good work done over the past years in cybersecurity awareness creation

efforts from a week-long to a month-long celebration. He mentioned that his presentation centred on how COVID-19 has affected compliance activities and some of the key things that ought to be looked at to ensure that the baseline of compliance is not affected. He started by defining what compliance is while indicating that it could be achieved through organisations keeping their operational integrity by ensuring that all the things needed to keep businesses aligned are done successfully.

The four main requirements for compliance he said, are legislation (Electronic Transactions Act, Electronic Communications Act, Data Protection Act, etc.), regulation (Bank of Ghana (BoG), Cybersecurity Directive), industry standards (ISO 27001, NIST, PCI-DSS, etc.) and the company’s policy and contracts signed with other organisations. He mentioned that if the Data Protection Act was being implemented effectively, we would have a lot more organised and structured environment within Ghana. He stated that it is very key that legislation is correct and aimed at achieving the right objectives to make it effective. He further added that regulation is difficult and since the BoG released the regulation for the banking sector in 2018, no other regulatory body has released any regulation and that is a major concern. He added that the expectation was that since one regulator has established an Act to ensure that their sector is organised, it will trickle down to the other regulators of other sectors. He stated that it is key that this is done because it is from a regulator’s perspective that the right requirements or

provisions of regulations can be implemented. He mentioned that if an organisation wants to be at their best, it is crucial that they look at the best practices, standards and frameworks for their industry and adopt them. He went ahead to state that real compliance manifests at the company policies and that it is expected that company policies take inputs from legislation, regulation and from industry standards when being developed. Additionally stated was how COVID-19 has come to create additional problems in cybersecurity, and opportunities in the increment of the following; Malware/Phishing, Social engineering/scams, hacking and WFH-teleworking. He mentioned that true compliance happens at the middle level of management (Operations/Compliance/feedback). Engagement is being lost by working from home because there is a significant lack of direct interaction, there is a sense of departure from the line manager and the workforce, and hence there is a slow gradual weakening of the compliance regime within organisations. He shared that values and messaging, ethical decisions, creating a safe space and developing managers to lead; are all tones at the middle management, adding that the tone at the middle is critical to ensuring that the right structures are established to ensure compliance. He concluded by highlighting that the use and application of a framework is essential for any organisation as the characteristics of any framework are the organisation, its structure and ensuring that processes are well-formed and integrate with each other easily. He proceeded to say that, COVID-19 has disrupted the

organisational environment and so if the culture of the organisation is not well organised, then the response to all these changes become difficult and compliance levels become lower.

Presentation By Sponsors Margins Group



The next presentation was done by Mr. Yabuko Abdullai of Margins Group. Mr. Yabuko Abdullai started his presentation by introducing the Margins group as a dynamic company, whilst elaborating on the history of the company. He took the audience through the various transitions of the company and concluded that, in 2012, the company became a Special Purpose Vehicle (SPV) engaged in a Public-Private Partnership (PPP) with the

National Identification Authority to provide foreigners in Ghana with a non-citizen Ghana card.

Tenece Professional Services Limited



Mr. Jonathan Dartey of Tenece Professional Services Limited presented next. Mr. Jonathan Dartey stated that Tenece Professional Services Limited has been at the forefront of driving cybersecurity infrastructure and application solutions in Ghana since its inception 12 years ago. He mentioned that the company started in Nigeria and has a presence in Ghana, and over 23 other African countries. He stated that the government has done a lot in digitalising the economy, but digitalisation has some inherent problems noting that email threats have risen exponentially within the last 12 months. He expressed concerns of customers who have some challenges around the implementation of a point solution, management of point solutions especially as CISOs are having to look at budget cuts within the

context of COVID-19. He shared that there are questions that users of IT infrastructure need to ask in order to stay ahead of the threat landscape. Questions worth asking are; the assets they have, how critical they are, who can access them, what services are being used by their employees, how they connect to those services, and many more. He then mentioned that this is how Tenece comes in to aid in changing the approach or the strategy. He discussed the information systems security solutions that Tenece has to offer which includes; perimeter security & access control, data protection, encryption, masking, application protection, cloud security, next Gen SIEM/SOC/ Security Audit among others. He ended his presentation by sharing that, zero trust must become the new standard wherein no one and nothing is trusted by default. He also encouraged companies to reduce risk by 85% by signing on to their free CIS Controls package from now till the end of the first quarter of 2021.

CalBank Ghana

Mrs. Martha Acquaye, the Head of Financial Inclusion at CalBank Ghana gave the next presentation. She indicated that her role involved the use of digital channels to drive inclusion adding that inclusion has moved past unbanked and underbanked but that gender is currently being considered. She then went ahead to speak about delivering a robust digital banking solution by stating the characteristics of a robust digital solution. She made



reference to the Deputy Minister for Communications with regards to the financial sector being a target for cybercriminals during the COVID-19 era. She confirmed that indeed the sector has been a major target and CalBank has put in place measures to protect the bank and its customers. In continuation, she went on to describe what a robust solution was, noting that a robust solution is a solution capable of facilitating a very comprehensive customer identification and verification process with strong authentication procedures. She mentioned some initiatives CalBank had put in place to ensure the protection of the bank and its customers. Some of the initiatives included regular security reviews, staff training on security issues (which she stated is the first level of security because it ensures their staff leave fewer gaps), system encryption, PCI-DSS compliance and ISO 27001 certification. She then introduced the audience to some of their products which included; an alert solution for transactions, 3-D secure, cards which are chip and pin-based, mobile banking applications, internet banking, payment platform, agent banking services, and SNAP

(designed to attract the unbanked). She emphasized that as a bank they continuously work on their security protocols to ensure that they protect the bank and its customers. She concluded by stating that CalBank is passionate about security and delivering a good customer experience.

SpearHead Networks



Mr. Ernest Darko Mensah, the Managing Director of SpearHead Networks was the next to present. He began by taking the audience through the history of the company stating that the company was established in 2007 and has partnered with over 300 cyber technology giants in the world. Through these partnerships, they have succeeded in taking down accounts, criminal activities and vulnerabilities using the Zerofox tool. The tool also aids in taking down impersonating profiles, malicious sites and rogue mobile applications. The platform enables the protection of critical digital assets, by detecting, analysing, optimising and disrupting

harmful cyber activities across all platforms. He concluded by taking the audience through their breach and attack simulation tool which safely executes thousands of proven breach and attack simulation scenarios across the entire cyber kill chain automatically, continuously, and at scale to determine where security is working as expected and uncover areas where specific attacks will break through current defence configurations. The purpose of this is to validate and improve security controls he added.

Maryland and Mr. Gabe Goldhirsh of Zerofox who joined virtually. The moderator for this session was Mr. Albert Yirenkyi Dankwah of Stanbic Bank.

by the pandemic and they will use the session to discuss business continuity plans, operational and monetary challenges when it comes to cybersecurity.

Proceedings



Discuss how units were mobilised in March to enable the business to continue during the pandemic.



Panel Discussion COVID-19 & Cybersecurity

The panel discussion on “COVID-19 and Cybersecurity” continued next after the health break. The panelists were Mr. Nana Kofi Asafu-Aidoo, the Executive Director of the Ghana Domain Name Registry who joined the session virtually, Mr. Michael Kwofie of the Standard Chartered Bank, Mr. Eric Akwei of Surfline Ghana, Marcelle Lee of Secure Works who also joined virtually from

Mr. Dankwah welcomed the audience to the session and introduced the topic for discussion. He mentioned that discussions would focus on how cybersecurity has been affected by COVID-19 and how to use cybersecurity to enable business processes during this pandemic. He mentioned that industry players were most affected

Mr. Kwofie → Standard Chartered Bank, is fortunate to be working as a group and most of the preparations started before March. He mentioned that other parts of their franchise had been affected by the pandemic and some simulations had started in February in anticipation of a lockdown. He mentioned that they had some infrastructure in place and the bank was practising work from home (WFH) policy. He also added that zero trust had to be considered and that it was pertinent that the end point and the user become the new perimeter. He mentioned that for the WFH policy to work efficiently, the user’s computer and mode of access had to be secure.





How was your team mobilised to deliver during the pandemic when data usage was at its peak?



Mr. Akwei → There was a huge surge in traffic and when this happened, they monitored the capacity of system resources to ensure they could meet the demand. He mentioned that the advantage that Surfline had was that its infrastructure was built to handle twice the capacity.



What did you see differently, from Ghana Domain Name Registry (GDNR) point of view, during the pandemic?

Mr. Asafu-Aidoo → The Ghana Domain Name Registry (GDNR) witnessed a rise in registration of domain names especially “.gh” domain names. He added that many businesses moved online during the pandemic.



What was the rise in registration of domain names and how was the GDNR able to differentiate between legitimate and illegitimate domain name requests?

Here Mr. Asafu-Aidoo indicated that at the point of registration, there was no real way of determining whether registration was legit or not. He mentioned that they were able to differentiate this after registration when the person uses the site for fraudulent activities, and that was when an officer of the GDNR follows up to take the sites down. He also mentioned that post-registration, there is a kind of monitoring process and reports are consequently sent to the cybersecurity reporting platforms about particular sites.



Give your perspective on some of the occurrences from a global point of view.

Madam Marcelle Lee → From a threat intelligence perspective, it did not take the threat actors very long to jump on the COVID-19 train and start using it as a lure for all kinds of different activities.



From an infrastructure point of view, what was done to protect the digital infrastructure of Surfline?

Mr. Akwei → There has been an implementation of various security tiers that allow clients to connect through the network at various stages. Every tier has several security protocols, however, as a company, challenges have been experienced with individuals using their personal machines for work at home. This is because the personal machines do not have security controls installed on them and so makes them vulnerable to cyber-attacks. He also mentioned that their interaction with the NCA-CERT has been beneficial because

the CERT shares information on vulnerabilities with Surfline Ghana which helps them put in place the right infrastructure and controls to guard against cyber-attacks.



Standard Chartered Bank's Perspective

When asked about the structures Standard Chartered Bank had to put in place during this period to ensure the security of customers, Mr. Kwofie said that they had some discussions with colleagues in the industry focusing on three main issues; raise in social engineering which can give room for an incident happening within the bank and also to the customers, the use of communications channels and the need for staff to work from elsewhere due to social distancing. He admitted that although technical controls could be implemented in some situations, they realised that some of the solutions available were more dependent on the behaviour of staff and customers. He mentioned that they however managed to ensure that their endpoints were secure; staff were connecting via Virtual Private Networks (VPNs) and correctly, data loss prevention controls and security monitoring (knowing what happens at different times of the day) controls were implemented. He stated that determining acceptable behaviour while working from home seems to be a major challenge. He also mentioned that certain applications were introduced on the go and because of the time constraints, these applications were not assessed carefully and in effect presented two issues; introduction of vulnerabilities into the organisation's whole setup and deviations that could not tracked.



What are some of the challenges that stood out during this period and were they resolved?

Madam Marcelle Lee → There has been a variety of different problems from this sort of surge in remote work. She mentioned that a lot of it comes down to endpoint controls giving some specific examples of a worker working from home who is connected to the company's VPN and also connected directly to the internet for surfing. She mentioned that they have seen instances where on the unprotected side, the host was communicating with a remote command and control server and that was not detected because it was not going through the VPN and appropriate network. She also mentioned that multifactor authentication being included in VPN connection is ideal and has the potential to stop threat actors from getting into the system. Mr. Dankwah then asked the panelists to respond to this, that since working from home has become the norm, there are a lot of tactical decisions and controls which were not part of the strategy but had to be implemented to enable the business to go ahead.



How do we ensure that we don't leave these tactical controls to run perpetually but we will be able to take them out while we are easing back into full operations?

Mr. Asafu-Aidoo → Due to the situation, meetings had to have more consistent dates and times and they had to standardise digital communications media.

He mentioned that going forward, there is still going to be more virtual communications and it's important that a lot of lessons are taken from this period for application into the new way of working which is the new normal. He also mentioned that we have to have a new respect for data (the storage of data; making sure that data sitting in servers are encrypted and also data in transit is also encrypted) to prevent them from being intercepted during virtual communications.

Mr. Akwei → It is necessary that critical data is secured. He mentioned that backups must be very secure, systems that connect remotely should be properly authenticated (multifactor authentication) and there should be monitoring procedures in place to trigger system alerts.



From an organisational point of view, how was the transition from traditional organisations to digitised institutions going to stand the test of time?

Mr. Kwofie → In terms of digital transformation, any organisation that is still operating today has moved ahead five years of its time and had probably been thinking through it but never had the boldness to be able to implement it. He gave an example of schools which are running online classes. Adding that business continuity practices should be made more resilient and scenario-based and also, decisions taken during the lockdown should be reviewed to formalise those that need formalisation. Madam Marcelle Lee's response was that currently, the attack surface has increased because

many organisations are going online, and some are being attacked not by sophisticated threat actors but by students who for instance do not want to go to school and want to disrupt online activities. She also mentioned that proper security measures have to be implemented across the board for different organisations for efficient work from home.

Mr. Asafu-Aidoo → Organisations that are currently not virtual will take some time in managing the environment and will need help especially in setting up the security and operational aspects adding that such organisations should collaborate with institutions that have experience in this field to prevent making certain basic mistakes that could cost them more than they expected.

Mr. Akwei → Organisations need to partner with seasoned organisations to know what works in the space.



How to bring third parties on board to be able to support them to prevent them from presenting some threats to business?

Mr. Kwofie → When it comes to onboarding a third party, it required a security assessment, to ensure they meet security policies and support them in areas where they don't meet your requirements. He mentioned that the Standard Chartered Bank had to do a quick review of their third parties. He also mentioned that third parties be included in information security training and should be made to understand how information and data flows must be secured end to end.

Madam Marcelle Lee → It is necessary to have the Service Level Agreement with them by being clear of who is providing what, and having meaningful programmes incentivising users to make the right decisions versus penalising them for not making the right decisions.



What challenges are likely to be faced in this new era of moving operations digitally?

Mr. Akwei → An attack is more expensive and so it is pertinent that the necessary security controls are in place to fully operationalise digitalisation. He mentioned that as a service provider when selling solutions to customers, many add-ons are provided in terms of security and backup solutions. However, it was realised that when this is being presented to the potential customer, they prefer not to include the add-ons which are critical to secure data and communications. He added that this gave them a sense that the business community has not fully understood the risk that is to be faced if they do not fully adopt this security posture with businesses. He mentioned that it is necessary to take this seriously and educate staff on security. Management should also be aware of some of the impacts of not applying the necessary security controls and investments in securing systems, in order to save the business from losing money to cybercriminals.

Mr. Asafu-Aidoo → A lot of challenges encountered compromise on cybersecurity of organisations and that there should be a way to share resources between small, medium and large organisations to ensure

that systems are secured at all levels to prevent data leaks. He added that this will prevent small organisations from being the weak gate into the big castle. He also mentioned that training is crucial and should not only be concentrated on the skills, or awareness in spotting a bad link in an email or seeing a phishing website but it should be about the attitude towards cybersecurity. He added that a shift in the paradigm of work will also be a challenge because currently there are no mechanisms in place to determine if people working from home are actually working as expected. He also mentioned that digital literacy is also a challenge because in Ghana those who know about doing things virtually are IT personnel, and so there is a need for ongoing digital literacy training across professions, several demographics, age groups, and gender. He finally added that data is also a challenge because many organisations are storing data on the cloud and so storage location is a concern. He recommended that the Government of Ghana set up more data centres in Ghana because the legislations in Ghana cannot apply to data stored outside.

Mr. Kwofie → This situation will cause lots of children-related challenges because most children were home and were also accessing the internet. It will therefore require some investment to fully secure devices at home and this may be a challenge for some. For small and medium scale enterprises (SMEs) it will be necessary that investors get the right skill to aid in risk assessments to get the right controls in place. He mentioned that investment does not always require money because, for every tool, there is a cheaper version

or an open-source version that can help in achieving similar objectives. He mentioned that organisations need to pay utmost attention to the governance around cloud adoption and in moving data to the cloud, in addition to taking cyber hygiene practices seriously so they can appreciate the need for cybersecurity.

Comments from Audience

Mr. Alex Ntow of EITBS indicated that one of the things that organisations fall short of is the senior management reduced involvement in cybersecurity discussions. This as well as views on what needs to be done with regards to cybersecurity is totally different and this brings a lot of problems especially when it comes to funding for cybersecurity. He recommended that heads of agencies be trained on the impacts of not having security in place and cybersecurity breaches so the need for cybersecurity is much appreciated. In addition to the point made by Mr. Ntow, Mr. Dankwah indicated that the pandemic has made cybersecurity come to the forefront in almost every discussion in boardrooms. He mentioned that this pandemic may help in navigating one of the challenges when it comes to budget constraints. He added that he looks forward to the Cybersecurity Bill being passed because its long overdue. To conclude the session, Mr. Dankwah thanked the panelists for a fruitful discussion and then thanked the audience for their cooperation during the discussion. Over 6.6 thousand people were reached via the Facebook pages of Citi Fm and YEN.Com.

ROUNDTABLE DISCUSSION

Embracing Change and Digital Transformation in the Era COVID-19



As part of the National Cyber Security Awareness Month (NCSAM) 2020, the National Cyber Security Centre (NCSC) hosted a roundtable workshop on Tuesday, October 20, 2020, at the Accra Digital Centre to deliberate on the increasing rate of digitalisation owing to the COVID-19 outbreak and how the world is embracing this new way of life. Madam Jemima Owusu-Tweneboah of the NCSC formally welcomed the dignitaries, and all organisations present while highlighting the purpose of the workshop.

Welcome Address

The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako in his welcome speech, stated the increased rate of ICT has resulted in jobs losses. Dr. Antwi-Boasiako reiterated that the financial

sectors had resulted in branchless banking due to digital banking which has resulted in a reduced need for in-branch staff. Dr. Antwi-Boasiako outlined the law of energy conservation which states that energy cannot be destroyed but can only be transformed from one form to the other, indicating that jobs are not being lost but being transformed hence the need to take advantage of the changes occurring.

He also highlighted the big themes that underline Ghana's digital transformation which included Artificial Intelligence (AI) such as driverless vehicles, drones, machine learning systems and robotics. There was also blockchain technology that has gained popularity in the financial sector and land administration as well as big data and other development that are dominating

the digital transformation space. For cybersecurity, these are the inevitable changes that are ongoing. He noted a wise saying that we do not control how the wind blows but as captains, we can only navigate in a way to take charge of the ship and get to its destination.

In conclusion, Dr. Antwi-Boasiako emphasized the need for a cybersecurity policy and strategy that will address these emerging threats as far as digital transformation is concerned. Regulation that comes from the cybersecurity legislation and regulates the use of artificial intelligence in ICT development and ecosystem. He added from the technical angle that we should be looking at security by design and how to build systems that are more secure.

Presentation By Sponsors

GrowForMe

The Chief Executive Officer/Co-founder at GrowForMe, Nana Agyemang Prempeh, emphasized an application called MyChurchPay where transactions are taken both online and offline and are passed on to the bank account which helped contribution grow by three times. From there, they came up with MyBusinessPay which is purely for customers to make payments to businesses. He then outlined the process of the payment system and how it works. According to Nana Agyemang Prempeh, the COVID-19 pandemic enabled them to go cardless. GrowForMe is a crowd funding and a crowd farming platform that makes it possible for one to farm. In conclusion, he stated that the integration of WhatsApp and Satellite into the farming system brought about an immense increase in farm productivity since one can determine the rain levels and temperature using the application.



Esoko

Mr. Xose Alijah from Esoko stated that the COVID-19 pandemic has made technology advancements a norm since children are now in the house and every parent has to figure out how to turn on the computer, connect to the internet, install “Zoom” and opening Facebook accounts. A lot of people have now joined digital platforms due to COVID-19 and this puts a lot of responsibilities on industry stakeholders. Esoko is a technology business that profiles people, collects data and help deliver services to underserved communities across Africa. In Ghana, Esoko has helped NGOs and Government to profile and serve over 4 million people and over 1 million farmers for advice and providing timely interventions for farmers to grow crops using their technology. Momo transactions in Africa has been on the rise from about 2.5% which is from 3 billion to 4.5 billion cedis. There was also a lot of increase in online transactions. The interesting thing in all this was the fact that working from home has become the new normal. When COVID-19 hit, the biggest headache was how to get people to work securely from their remote workstations. If you work in an office, you can shut down the network and put in place all the security principles to ensure a safe environment for working, but here is the case where you have been given a laptop to work from home without all the security measures you had at the office. All these advantages has made working faster and easier which also came



with some disadvantages. Esoko's line of work transformation meant they had to also improve on their working system. Their solutions and applications were based on agents who go to the field and profile people with an android held device. During the COVID-19 and consequent lockdown, they could not do this any longer and this was one of the challenges they faced. As Esoko is known for the powerful platform they had, they were able to work and profile millions of people within weeks. They had to figure out how to collect data without going to the field securely, but they were able to do this using their call interviews also known as KATI. They also faced a challenge where they were running a shift system, customers spoke to different people daily, hence a system was developed so the most immediate customer is called. This cut down repetition of people called. Change is a big challenge for organisations and COVID-19 has forced most organisations to have this change. For change to happen organisations need to invest more in training and also as individuals, there was the need for self-education as

not all is known. He also encouraged everyone there to work around for solutions.

Technosolve



Technosolve represents a global leader in cryptography and encryption named THALES. In his presentation, Mr. Robert Daniels indicated that most of the security being thought of is based on money. He went on to add that Thales is a global leader with 80 thousand employees worldwide in over 60 countries. Turnover last year was over 19 billion with specialisation in Hardware Security Model (HSM) and HSM based solutions. Its flagship product is a faced shield 8,000, 9,000 and 10,000 which is an electronic based transaction that comes from ATM and POS

transactions. There is also a specialisation in the general-purpose HSM called the THALES LUNA which has an inbuilt solution that deals with credentials like user identity, credentials management, data protection policy and key management.

He concluded with a video documentary that showed other services being offered.

The event saw the participation of 200 people physically as well as 2.2 thousand participants via the Facebook page of Citi FM and about 120 viewers on Youtube.

SESSION 2

Roundtable Discussion on Embracing Change and Digital Transformation



The discussion was moderated by Mr. Carl Sackey – ISACA Ghana. Panelists included:

- ➔ **Mrs. Jaqueline Hanson Kotei**
MTN Ghana
- ➔ **Dr. Kenneth Ashigbey**
CEO of Telecom Chamber
- ➔ **Mr. Carl Sackey**
Ghana Community Network Services Limited (GCNet)
- ➔ **Mr. C.K. Bruce**
CEO Innovare
- ➔ **Mr. Richard Okyere-Fosu**
Director - General NITA
- ➔ **Mr. Victor Addison**
Security Architectural Consultant



Mr. Carl Sackey touched on how we have moved from normal times to where we are currently. He asked a question about COVID-19, whether the pandemic was here to stay and the changes that have taken place since the beginning of the pandemic.

Dr. Kenneth Ashigbey opened the floor referencing what the telecommunication space has been and how prepared telecom companies were when the pandemic hit the nation. He shared the pressures that were brought on the telecommunications networks, expansion on the networks and the introduction of all the plans being enforced. He also touched on the fact that COVID-19 is not leaving anytime soon. One of the things COVID-19 has revealed the fact that it is not about the plan but more about strategies and resiliencies built with institutions. Another thing COVID-19 revealed is the need for teachers to learn how to use computers and for schools to equip teachers with computers to be able to work from home. He proposed a partnership between the private sector and the government sector in terms of



providing internet to underserved communities. He further said GIFEC has to change the role it plays in terms of providing access to the internet. The time has come where there is the need to change the whole communication structure. A note was made of what would happen if all the policies, 5G networks and IOT's were in place.

Mrs. Jaqueline Hanson Kotei continued with what MTN has also done to help in the transition to the new normal. She noted the introduction of WhatsApp lines for validation, social media platforms to interact with customers even after working hours. She further said that these platforms were in the pipeline, but COVID-19 accelerated the rollout



and its uses. She said COVID-19 has proved that working from home is perfectly fine. She admitted that the team needed more support in terms of emotional wellness and mental health wellness as a result of the change in environment. There was an increase in demand for cybersecurity with the new modes of operations. Therefore a lot of work needed to be done in their organisation because now the focus has shifted from their offices to homes and simulations to pre-emptively prepare for any potential cyber breaches are being seen as important. CERT is also important as the personnel are well-trained to be able to respond to incidents.



Mr. Victor Addison of the Security Architectural Consultant stated that customers are not able to drive out to transact business and having to result to an online transaction with some businesses having their website cloned. Further investigations showed that the fake sites were more secured than legitimate sites. The fake sites had SSL certificates but the legitimate sites didn't. The rise of cloud-based services and having a cloud-based database comes with its own challenge. Having a secured VPN for customers and how they are

accessing the data in a secure way and how the data are stored on base and in the cloud.



Mr. C.K. Bruce, the Chief Executive Officer of Innovare shared some points on the benefits of COVID-19 to Innovare. It has been interesting, but increased work has mostly been from the Bank of Ghana. From the acceptability point of view, Zoom has long existed before COVID-19 hit but Mr. Bruce indicated that he had to read more on it when the pandemic hit. "It is just that we didn't realise it works and can use it in so many ways" he added. He went on to state that Zoom is now being used for all manner of activities such as parties, naming ceremonies and including having serious meetings on zoom. The cybersecurity challenge with zoom is the issue of zoom bombing. He also encouraged awareness creation for the public and shared what one can do to be safe on zoom. Mr. Carl Sackey the moderator for the session thanked the dignitaries, and all organisations present for taking time off their busy schedule to join the meeting. He finally entreated all to make use of the available resources online to get themselves certified.

WORKSHOP ON ADDRESSING CYBER FRAUD IN GHANA'S FINANCIAL SECTOR



The recent fraud and cybercrime report by the Bank of Ghana highlights the increase of cyber-fraud and financial crimes stemmed from the advancement in 'cashless' banking products and services. Despite the decrease in the number of cyber-fraud cases from 174 in 2018 to 114 in 2019, the resulting loss in 2019 increased by 282% from GHC3.74 million to GHC14.31 million within the financial sector. This figure can only escalate considering the increased reliance on digital platforms for financial transactions due to the COVID-19 pandemic.

In recognition of the trend, the Bank of Ghana in its Cyber & Information Security Directive, issued a notice to all financial institutions to review and implement specific cybersecurity measures and controls to mitigate cyber fraud within the industry.

Indeed, the industry must recognise that security incidents are an ever-present risk and as such, in order for financial institutions to keep up to date with current and evolving threats, they must constantly formulate, implement and review cybersecurity policies, implement stringent technical mechanisms, conduct regular awareness training, adopt advanced authentication techniques among others to build a strong defence strategy in preventing and detecting cyber and financial crime incidents. Evidently, cybersecurity underpinned by proper risk management procedures, stringent recovery plan, good information security policy and strategy, incident management and response procedures, compliance and monitoring mechanisms and capacity building for staff has become imperative

to ensure the business continuity of organisations in this era. The workshop was expected to assess the risk-mitigating measures in dealing with the increasing cyber-fraud in the financial sector, assess the impact of cybercrime on the overall cybersecurity posture of the financial sector to proffer best business continuity and disaster recovery plans, deliberate on best cybersecurity measures to implement in order to address the rising financial sector cyber-fraud incidents, share industry experience on the various cybersecurity threats and risks being encountered by understanding the cyber threat landscape.

The event engaged representatives from member institutions of the Chartered Institute of Bankers (CIB) and commenced with opening

remarks by Dr. Albert Antwi-Boasiako, the National Cybersecurity Advisor. The National Cybersecurity Advisor stated that in line with the Ministry of Communications' strategy direction, the NCSC is going to improve the regulatory environment for cybersecurity. He stated that the draft Cybersecurity Act is going to establish the Cyber Security Authority that will have oversight of regulatory powers on cybersecurity matters in terms of directives, interventions and detection, awareness creation among others. He mentioned however that enforcement of the directive needs to be scaled up to ensure that financial institutions adhere to it. He added that the workshop was designed to help the conversation and collate best practices, the gaps and how we address them and importantly how to enhance collaboration and improve cybersecurity readiness within the financial sector. He welcomed the participants and encouraged them to share their perspectives and enjoy the session.

Madam Audrey Mnsi Mireku, the CERT Lead, thanked the National Cybersecurity Advisor for the opening remarks. She then introduced the Chief Executive Officer (CEO) of the Chartered Bankers Association, Mr. Daniel

Ato Kwamina Mensah who gave the opening remarks. Mr. Mensah began by thanking the NCSC for inviting him. He commenced his remarks by stating that cybercrime poses real and persistent threats to financial institutions of all sizes and the number of people who fall victim to cybercrime and digital espionage continues to rise. The financial services sector and its customers are also heavily targeted. The COVID-19 pandemic has brought with it a significant increase in fraudulent activities. He mentioned that working from home is now the hallmark of their industry and



has made their staff targets for cybercriminals. He mentioned that there is an increased risk with staff in the industry as well. This threat is what he called the hostile home network because multiple family members could be connected to the same network which could expose their devices to possible malware infections if their endpoints are not protected. He added that banks are now providing awareness to their customers on basic security measures. He shared that in an area where we have an elevated

consumer experience, consumers are more sophisticated and more aware and want flexibility in the services and products offered. As such, banks have responded very robustly in the area of digital banking and mobile banking which has given cybercriminals an opportunity to explore the various channels and attack the systems that have been put in place. He concluded that cybersecurity is of utmost importance to banks because their operations are more digitalised now and he admonished that greater emphasis is placed on cybersecurity in the banking sector. Madam Minsi

then introduced Mr. Philemon Hini of the e-Crime Bureau who then took the participants through the presentation "Addressing Cyber-fraud in Ghana's Financial Sector". The objective for his presentation was to assess the impact and risk-mitigating

measures in dealing with the increasing cyber-fraud in the financial sector, deliberate on best cybersecurity measures to implement to address the rising financial sector cyber-fraud incidents, share industry experience on the various cybersecurity threats and risks being encountered by understanding the cyber threat landscape, and lastly to expose participants to additional cybersecurity risks and discuss best practices. He began by taking the participants through the nature of

cyberspace. Cyberspace, he said, is a complex virtual environment, made up of the Internet, people, organisations, activities and networks that are connected to it. He added that for the use of cyberspace to prevail, stakeholders in cyberspace have to play an active role, beyond protecting their own assets. He continued that, safeguarding assets of interest is the responsibility of stakeholders who place value on those assets. An understanding of the risks on assets, threats, and selecting the controls to counter them and reduce them to an acceptable level is necessary. He added that to effectively address cybersecurity risks, industry best practices with the collaboration of all stakeholders, broad consumer employee education and innovative technology solutions could assist in addressing cybersecurity risks. He then added that the attack mechanisms fall into two main categories which are attacks from insiders in the private network and attacks from outsiders in the private network. Notable attacks on the financial sector include mobile money fraud, third party attacks, phishing attacks, malware attacks and insider attacks. He then talked about the role of the organisation in cyberspace which includes proper information security management by implementing and operating an effective Information Security Management System (ISMS), proper security monitoring and response, incorporating security as part of the Software Development Life-Cycle (SDLC), regular security education of users in the organisation through continuous technology updates and keeping track of latest technology developments, and sharing information with stakeholders on the current prevalent security risks. Mr. Hini also added that some controls against social engineering attacks such as basic policies governing the creation, collection, storage, transmission, sharing, processing and general use of organisational and personal information and intellectual property on the Internet and in cyberspace should be determined and documented, awareness and training, testing and two-factor authentication could be implemented.

A participant inquired that as a newly hired information security officer, what is the first task that is needed to be performed in the new role?

Mr. Hini responded by stating that in any environment, the first thing that needs to be done is to understand the environment you find yourself in, find out if the role already existed or it is entirely new. If the answer is that the role already existed, the officer is to find reports on implementation on things in there, have a stakeholder meeting and request historical information for review. He mentioned that this will enable the officer to appreciate the security controls that have been implemented to prevent the officer from trying to reinvent the wheel but rather build on what has been done.

It was also asked whether organisations should wait to be attacked by cybercriminals before coming up with controls to mitigate any further attacks or e-crime Bureau has the intelligence to assess the assets of the company and come up with controls to prevent them from future attacks.

Mr. Hini answered the question above stating that the company need not wait to be attacked first, rather they should do their risk assessment based on the service or the product they offer and then get the right controls in place. He also mentioned that there has to be periodic monitoring of all the company's assets to aid in the detection of threats. Madam Mireku queried Mr. Hini based on his assertion that antivirus is a thing of the past now, however noting that laptops and mobile devices are connected to work networks, she asked how these mobile devices are managed?

Mr. Hini answered that from an end-user perspective, an anti-malware or antivirus solution is appropriate but from an enterprise point of view, if you have an endpoint detection response solution it will perform the

action of antivirus and give you the capability to respond to malware appropriately. He mentioned that at a point in an enterprise's life, these attacks will happen, and they have to be ready and prepared to detect, respond and prevent attacks.

Madam Mireku then asked about securing "internet of things (everything)" devices that are used to connect from home. Mr. Hini answered stating that there was the need to put in place the recommended security controls on such devices as it directly exposes people to the internet. He mentioned that he separated his network to control this.

Madam Audrey Mireku then gave the next presentation for the session. She took the participants through the core functions of the National Cyber Security Centre which included incident coordination and response, awareness creation, guidance and advisory, research and development, policy and standardisation, and international cooperation. She then took them through the CERT Ecosystem which consists of the National CERT and the sectoral CERTs (National Communications Authority, National Information Technology Agency, National Security Council, Bank of Ghana, Industrial and

Commercial Systems, Academic and Research Networks, Military, Business or Private Sector). She continued by creating awareness on the Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC). Madam Mireku then discussed some cybercrime topologies (fraud, online impersonation, cyberbullying, misinformation, ransomware, service disruption, online child abuse, website defacement, DoS/ DDoS, Spam/ Phishing, Online blackmail, unauthorised access, malware, copyright information, publication of non-consensual intimate images among others) with the participants. She then went ahead to discuss the top incidents from the 11,545 incidents reported to the National CERT. Online fraud made up 65% of the reported incidents, publication of non-consensual intimate images was 19%, online impersonation was 12%, misinformation 3% and online child abuse 1%. She mentioned that lack of visibility, not enough collaboration with service providers, incorrect subscriber details are some of the challenges that the National CERT faced. She concluded by admonishing the participants to report all cybercrime incidents to the NCSC's reporting channels. She ended the session and thanked everyone for taking the time to attend.

WORKSHOP ON CRITICAL INFORMATION INFRASTRUCTURE (CII) PROTECTION AND RESILIENCE Part 1

Cyber-attacks on Critical Information Infrastructure (CII) in recent times is on the rise considering the over-dependence on technology devices and services. The magnitude, frequency and impact of these cyber-attacks on critical infrastructure are increasing and can impede the pursuit of economic activities, generate substantial financial losses, undermine public confidence and cause major damage to the economy. To help address some of these issues, the workshop convened participants who were representatives from each of the CII institutions in Ghana and aimed to enable them to outline the roles of designated CII owners, raise awareness on the protection of critical infrastructure and essential services and outline avenues to strengthen collaboration and information sharing in improving on cybersecurity and risk management approach. The event engaged representatives from the Critical Information Infrastructure (CII) Sectors.

Madam Molly Schaefer of the United States (US) Embassy in Ghana, begun by introducing everyone on the US team and shared their desire to ensure that every participant present leaves the workshop with a new view of the critical role of CII in cybersecurity. Ms Stacie Duhaney from MITRE Corporation then gave a brief introduction and overview of the programme. She extended her appreciation to the Government of Ghana, especially the NCSC and

the US Embassy in Accra for their extensive work. She shared that this was the first workshop that focused on critical infrastructure and includes participants from the Government and the private sector and added that cyber is a cross-cutting issue, hence, bringing together all participants will contribute significantly to Ghana creating a safe and secure cyber ecosystem and one that can help build a secure economy. She gave an overview of the MITRE Corporation and how the workshop aimed at bringing together critical infrastructure elements.

This was followed by a presentation by Mr. Frederick Kwakye-Mafo, Lead for Critical Information Infrastructure, at the National Cyber Security Centre, who shared that Ghana is drafting a critical information infrastructure directive. He indicated that the United States (US) has a similar directive which is the presidential order 136/30 which stipulates the protection of its critical infrastructure, whilst the EU has the Network and Information System (NIS) directive which stipulates baseline standards for critical infrastructure. In continuing, he further indicated that Malaysia, South Africa and Singapore, are examples among many others who also have CII directives. CII's are so vital to the nation that disruption could affect public health and safety. He gave an overview of what CII is and added that Ghana needs to identify what its critical information

infrastructure is – namely sectors and systems. He further gave an overview of how the directive came about and the provisions made in the Electronic Transactions Act. He added that it is clear in the Electronic Transactions Act (ETA) that the Minister responsible for telecommunications must identify the critical sectors. Additionally, a Gazette needed to go out so that owners of CII are aware that they form part of the infrastructure. He further shared that there are 12 sectors that have been identified and are subject to review and change as may be needed. Ghana previously recognised 10 sectors but two more have been proposed based on GDP and economic benefit, namely the mining and manufacturing sector. He further highlighted that Ghana has engaged several stakeholders within the CII industry. The National Cyber Security Technical Working Group (NCSTWG) he added has also reviewed the CII directive, along with international organisations like the MITRE Corporation and World Bank, hence the next step will be the operationalisation and launch of the directive. He proceeded to touch on the three sections of the directive, namely policy, technical and organisational measures, and incident reporting. In terms of policy, it is expected that all CII's will have some cybersecurity policy in place which is expected to be no different from industry standards and address data protection concerns. There also needs to be a person designated to address all

issues of cybersecurity governance, security monitoring (citing the example of the Uganda Mobile money attack where it took three days to detect the attack), training and capacity building, business continuity and risk recovery funds and so on. He then touched on the next steps namely the registration of CII owners, National Cyber Risk Assessment, Development of Risk Framework for CII and Engagement with CII owners, after which he gave opportunities for questions.

The next session featured a presentation on Ghana's Cyber Critical Infrastructure Protection by Ms Stacie Duhaney from MITRE Corporation. She touched on why there was a need for Cyber Critical Infrastructure Protection. She shared the first steps of identifying critical information infrastructure and acknowledged Ghana's steps in identifying these sectors, as it would be difficult to protect something if we don't know its value. She reiterated the need to not only focus on national security and defence issues though that is important but also focus on elements like the economy, sovereignty alongside National Security when it comes to critical information infrastructure. Hence, Ghana adding mining and manufacturing to its CII is commendable because these are important parts of Ghana's economy. She added that for CII is also important to look at all the opportunities such as building a workforce that come with cybersecurity, adding that cyber protection is needed to harness some of these opportunities. Additionally, cybersecurity can either be an enabler or a hindrance to the things that need to be done

in governance. She further touched on the need for the public and the international community to understand a nation's values and how to work together. Since cyber issues can move to the technical side easily, the importance can be missed by the public, hence having the directive can help outline what a nation values and how sectors of the economy can work together for the greater good. Finally, there was also the need to minimise threats spreading to other CII sectors through information sharing and collaboration. She also touched on why it is important to codify information in law or directives, some of these include ensuring that everyone involved understands the necessary baseline protection and best practices as far as securing and ensuring roles and responsibilities. If there is an informal network, certain sectors may not understand what they need to do and how they need to protect their system, all of which are included in the directive. It also outlines who to respond to in terms of an attack, making it easier when something inevitable happens and further builds public and international confidence in the system. She further gave an overview of Ghana's cyber threat landscape, namely routine threats such as ransomware, organised crime, insider cyber-enabled crime, resiliency issues and physical threats such as cable cuts and natural disasters. She then proceeded to give an overview of the importance of Cyber Critical Infrastructure and ICT Vulnerabilities, how they occur and the main vulnerability categories, in addition to highlighting cyber risks and what they entail, and critical infrastructure resiliency among other salient topics related to CII protection. Subsequent to which she conducted

an exercise on Ghana's Critical Infrastructure followed by some questions from the participants. To conclude the session, Ms Stacie Duhaney thanked everyone for taking time to attend and shared that she was looking forward to engaging everyone present through other platforms such as workshops. She also thanked the CII team from the National Cyber Security Centre, participants and the MITRE team and added that she looked forward to more collaborations. About 30 participants of CII owners participated in the event.

WEEK FOUR

GOVERNMENT FOCAL AREA



CYBERSECURITY
IN THE ERA OF
COVID-19



NATIONAL
CYBER SECURITY
AWARENESS MONTH

NATIONAL CYBER RISK ASSESSMENT (NCRA) WORKSHOP Part 1

The pandemic has led to rapid digital transformation globally which is required to improve the functions and efficiency of public and private organisations, as well as the well-being of populations. However, the growing threats and risks facing global cyberspace and digital networks, information systems and data can significantly reduce the expected benefits, and seriously harm the interests of nations, their economies, institutions, and people. In this regard, the National Cyber Security Centre (NCSC),

in collaboration with the United Kingdom (UK) Government, via the Commonwealth Cyber Programme and the UK's National Cyber Security Programme, organised the National Cyber Risk Assessment (NCRA) Virtual Workshop to deliver cyber risk assessment training for Critical Information Infrastructure (CII) owners. The workshop was to help CII owners identify and assess the growing risks in cyberspace to critical information infrastructure. The event engaged representatives from the Critical Information

Infrastructure (CII) Sectors including MTN Ghana, MainOne, Volta Aluminium Company, National Health Insurance Authority, Margins Group, Copyright Office, Surflife, Lands Commission, British High Commission, Ghana Armed Forces and Comsys Limited

Welcome Address

Dr. Albert ANTWI-BOASIAKO
National Cybersecurity Advisor

In his opening remarks, Dr. Antwi-Boasiako indicated that the workshop was a build-on to an earlier workshop that took place and as such stressed that the workshop was to build capacity to help deal with issues relating to Critical Information Infrastructure (CII). He also made mention that the concept of the National Cyber Risk Assessment was introduced during a study visit to the UK. In his submissions, he expressed appreciation to the UK Government for their support around CII Protection. To address the risks that Ghana faces, Dr. Antwi-Boasiako indicated that there are multiple tools and processes that are used to address risks. He stated that Ghana's

cybersecurity development is in the formative stage and as such needs to take advantage and apply different methods and then choose the best one, or in some cases, customise its own methodology to address Ghana's risk associated with CII. He also added that the adoption will help Ghana to understand its own infrastructure, the interdependency and vulnerabilities around CII which will help in the categorisation of CII assets. In concluding his remarks, he indicated that information sharing constitutes an important element of the CII community and for that matter, CII owners need to interact and share information to address some gaps within the CII sectors.

Remarks

Mr. Thomas HARTLEY
Deputy High Commissioner, UK
High Commission, Accra

Mr. Hartley began by expressing his pleasure to be part of the 2020 edition of the National Cyber Security Awareness Month celebration. He stated that COVID-19 has driven innovation very quickly, however, cybercriminals are using this current crisis as an opportunity to exploit weaknesses in cybersecurity. He further stated that cyber technologies in the wrong hands can be used to disrupt lives and the WannaCry ransomware attack in 2017 which affected 150 countries shows how real the cyber threats are. He stated that it is a constant battle with cybercriminals but the frontlines in cyber operations in the Critical Information Infrastructure

companies and the key to success is working together. The collaboration between government, businesses and academia will reduce the threats posed by cybercriminals. He also added that the only responsible response is to build collective defences, and this was why workshops like the NCRA workshop are very important. Lessons learnt must be shared amongst all stakeholders to stand a chance of securing critical systems. He concluded by stating the NCRA captures this learning and focuses on improving the cybersecurity of Critical National Infrastructure. He ended by stating that the UK Home Office was happy to share knowledge on NCRA but are also looking to learn from the experiences of the participants.

Overview of NCRA Process

Jeremy Ketteringham
ICT International Directorate,
UK Home Office

He began by welcoming all participants and outlined his background which is in Cybersecurity Capacity Building and indicated that he had been delivering the National Cyber Risk Assessments for the past three (3) years. He stated the process has been used successfully in over 300 organisations worldwide, including four (4) African Commonwealth countries. The process is designed to hand over the tools, knowledge and skills to the local team. The objective is that at the end of the complete risk assessment process,

the local team have all the skills and information required to carry out another risk assessment process on their own. Cyber threats to Critical Information Infrastructure (CII) are growing in parallel to the digitisation of services. For nations to tackle this problem, there has to be an understanding of the cyber risks to CII, to ensure effective mitigation. Understanding what infrastructure should be considered critical, what essential digital services exist, who owns them and where they sit within the overall priority view of a country's CII. The risk assessment is focused on estimating what the impact of a disruption will be to each of the services.

There is a need to know how to defend against attacks but also how to respond when an attack occurs. The risk assessment begins with an interactive self-assessment survey to gather information on threats, impacts and vulnerabilities of the systems that make up the CII. The Risk Assessment is a repeatable process to track how the risk is changing and how effective some of the measures have been. Finally, it is designed to analyse cyber risk using tools to visualise the national risk picture. The NCRA is built around a risk management cycle, Measure, Analyse, Prioritise and Act. It identifies risk and their mitigations which helps identify strategic investments and kickstarts cyber improvements. The NCRA will inform Ghana's National Cyber Security Strategy, assist in the development of Ghana's Cybersecurity investment programme by implementing strategic capacity building projects and create risk dashboards, measures and metrics to measure

progress towards mitigation success. He ended by highlighting various platforms and capacity development programmes developed by the UK Home Office such as the Cyber Information Sharing Platform (CISP), a platform for organisations to share information about cybersecurity threats and also Cyber Essentials which is a simple and low-cost cybersecurity standard that many organisations who lack the budget to gain high-end certifications can sign up for.

NCRA Questionnaire Walkthrough

Andrew CAMERON
ICT International Directorate,
UK Home Office

Mr. Cameron commenced his session by displaying a questionnaire and introducing the different sections of the questionnaire. The explanatory notes section gives a detailed overview of the NCRA Questionnaire, the Organisation Questions section which gathers details about the organisation undertaking the assessment, the sector which they fall under, the critical systems in the organisation and the prominence of cybersecurity within the organisation, the Systems 1-10 section which gathers information about the threats, impacts and risks pertaining to each system identified in the organisation Questions and the Systems Summary section which captures all the information from the other sections into one to be analysed by the Data Analyst.

Mr. Cameron then proceeded to fill out the questionnaire with data of a fictitious company to demonstrate the information required for each section. He concluded by displaying the Systems Summary section to show how a completed questionnaire should look like.

Remarks

Mr. Frederick KWAKYE-MAAFO NCSC Critical Information Infrastructure Protection Lead

Mr. Frederick Kwakye-Mafo began by thanking the UK Home Office team for the presentations. He then went ahead to give the participants and CII Owners assurance on information sharing. He highlighted the roles and persons responsible with regards to the NCRA process according to a Responsible, Accountable, Consulted and Informed (RACI) chart provided by the UK Home Office team while indicating that Hon. Ursula Owusu-Ekufu, the Minister for Communications has been a champion for cybersecurity. The Head of the department role will be played by Dr. Albert Antwi-Boasiako, the National Cybersecurity Advisor; the team lead for the engagement will be Mr. Frederick Kwakye-Mafo, Critical Information Infrastructure Protection Lead; the Organiser role being Madam Audrey Mnisi Mireku, Computer Emergency Response Team Lead of the NCSC; the Cyber Expert role will be played by Madam

Jemima Owusu-Tweneboah, Cyber Analyst and the Data Analyser role being Mr. Gerald Awadzi, Cyber Analyst. He continued to give assurance on how data received through the NCRA questionnaires will be stored and secured. He stated the NCSC recognises that the data collected is highly sensitive, not only to the organisations in question but also to the country, so commensurate security measures have been put in place to protect it. He highlighted the existence of a secure portal for the exchange of such confidential information, the Trusted Information Sharing Network (TISN). The CII Owners will have to register to have access to the TISN. The TISN will also facilitate the training and capacity building of the CII Owners. He concluded by requesting for questions from participants. Mr. Gerald Awadzi concluded the workshop by expressing gratitude to all the participants for honouring the invitation and special thanks to the UK Home Office team for the knowledge transfer. He finally requested the participants to send an email with their contact information and the institution they represented to info@cybersecurity.gov.gh to foster communication and relationship building.

WORKSHOP FOR SECTORAL COMPUTER EMERGENCY RESPONSE TEAMS (CERTS) ON LESSONS LEARNED IN THE ERA OF COVID-19 - Virtual Platform

As part of the National Cyber Security Awareness Month 2020, a workshop was organised for sectoral Computer Emergency Response Teams (CERT) on Lessons learnt in the Era of COVID-19. This was a workshop organised to create the platform for the various components of the CERT-GH Ecosystem to share experiences on the kinds of attacks experienced during the era of COVID-19 and to discuss best practices and possible mitigatory measures that can be put in place to deal with prevalent trends within the various sectors. The workshop was held on October 23, 2020 on a virtual platform (Zoom) that allowed for a meeting with the various stakeholders of this event.

The officers from the following institutions participated in the workshop;

- ➔ The National Computer Emergency Response Team (CERT-GH)
- ➔ National Communications Authority CERT (NCA CERT)
- ➔ National Information Technology Agency Security Operations Centre (NITA SOC)
- ➔ Ghanaian Academic and Research Network CERT
- ➔ Military CERT
- ➔ National Security Council CERT
- ➔ Industrial and Commercial System CERT
- ➔ Business and Private Sector CERT
- ➔ Criminal Investigations Department
- ➔ Data Protection Commission
- ➔ Bank of Ghana Security Operations Centre (BOG SOC)

The event began at 2:00pm local time. Participants were asked to pre-register and were admitted into the live online session by the virtual platform administrator. The moderator kickstarted the event with an opening prayer.

Welcome Address

Dr. Albert ANTWI-BOASIAKO
National Cybersecurity Advisor

The National Cybersecurity Advisor in his remarks appreciated the effort of some people who have been a lot of help to the CERT-GH team. He then identified some of the public sector CERTs that have been involved in a lot of activities such as digital services like the National Communications Authority CERT, National Information Technology Agency SOC, Military CERT and others. He pointed out that in October 2019, the Minister for Communications launched a Cybercrime/Cybersecurity Incident Reporting Points of Contact (PoC) for easing reports and it has been a massive success. From January 2020 to August 2020, more than 11,000 contacts were made with the national CERT. He commended the national CERT team for contributing significantly to this success. The work of the national CERT team has prevented about 5,000 Ghanaians from falling victim to cybercrime.

The CERT-GH team has also done very well by giving support to law enforcement agencies. CERT-GH has

also achieved several results by way of advisories, alerts and guidance that has been given to the public in preventing cyber fraud and other cyber activity issues. He updated them on recent happenings to improve the cyber ecosystem. The National Cyber Security Centre, he added is developing the state of cybercrime and cybersecurity report of the various cybersecurity incidents happening within Ghana. He again mentioned that the World Bank is also supporting the deployment of platforms (infrastructure) to help the communities in terms of information sharing of incidents and advisories. CERT-GH, he also indicated will also have a mechanism of sharing information in a timely manner with the various communities and constituents adding that in all these activities, capacity building is key. He, therefore, encouraged everyone to share experiences and leverage what participants will share to build a strong community. He concluded by asking everyone to stay motivated and work hard together to ensure the safety of the cyber ecosystem in Ghana.

Presentation

Mr. Eric AKUMIAH
Ministry of Communications,
E-Transform Consultant

Mr. Eric Akumiah in his presentation gave a historic perspective about how information sharing on incident handling was and its

current status. He spoke about the origins of the CERT-GH in Ghana and the journey to start a national CERT. He stated that some key private and government sectors were invited to send representatives to engage with NITA on establishing an incidence response mechanism which was non-existent in Ghana at that time. A National Computer Emergency Response Team (CERT) was established under the National Information Technology Agency.

Development of an operational framework for the national CERT, determining the stakeholders to be involved with national CERT and the roadmap for the development of national CERT were some of the terms of reference of the CERT national steering committee that was set up. He stated that a number of meetings took place between August 2010 and an important outcome of these meetings centred on the Ministry of Communications to assign NITA to set up the government CERT and the Ministry of Communications to develop a national CERT. He further stated that a series of high-profile incidents experienced by the government in 2014 mandated the formation of the unit to investigate cybercrime issues. He stated that the team started with 2 members while elaborating on the various steps taken by the government to make sure that Ghana was collaborating effectively with relevant international bodies to reduce cybercrime and handle cybersecurity issues. In his closing statement, he elaborated on the various achievements of CERT-GH from 2014 to date.

Presentation

Mr. Francisco FONSECA
Vice President and General Manager
National Cybersecurity for BitSight

Mr. Fonseca in his presentation spoke about an overview of the threat landscape of West Africa and exposed the audience to the various metrics used by BitSight for credit rating. 250-640 are the basic (poor), 640-740 are intermediate and then 740-900 are the advance (excellent). These ratings are not on the basis of objective matter or questionnaires; they are based on data. He also stated the steps by which the BitSight ratings are calculated. He showed Ghana's overview and its rating noting that Ghana's rate is 500 and that compared to other African countries, Ghana is relatively doing well. He then further elaborated on Ghana's key sectors and comparatively analysed the various levels of threats faced by the major sectors in Ghana's digital ecosystem. In his closing statement, he showed a chart of organisational distributions and how some organisations are performing better than others.

Sharing of Experiences (Lessons Learnt)

In this session, various presentations were made by the various sectors and this detailed their experiences in terms of cybercrime and how they have coped with their various challenges.

National Communications Authority (NCA)

There was a slide presentation by Mr. Kwadwo Osafo-Mafo, the

Director of Cybersecurity at the NCA. He stated that the National Communications Authority (NCA) CERT was inaugurated on October 22, 2018 by the President and the Honourable Minister for Communications. Now the National Communications Authority does not only look out for cybersecurity but also digital sectors. He again mentioned that the NCA-CERT is now part of the AfricaCERT. He emphasized how the NCA had to learn from best practices worldwide to conclude his presentation.

National Information Technology Agency (NITA)

Mr. Kwaku Kyei Ofori, the Deputy Director-General of NITA gave a speech on their experience with computer emergency response adding that in 2017, NITA started the implementation of the rollout of the SmartWorkplace Project. He elaborated on the measures NITA put in place to help in the era of COVID-19 and how these measures have supported the government sector and government businesses as well. He later concluded his speech and educated everyone on how they have fared during this period.

Data Protection Commission (DPC)

Dr. Patrick Adonoo, the Director of Regulations and Compliance, gave a speech on lessons learnt from the Data Protection Commission and how they have also fared. He stated that the COVID-19 pandemic has pushed the Commission to review its engagement with the public. The period gave them the time to

retrain staff and certify as many as possible. He elaborated on how the data protection amnesty works. He again stated that the operations of the Data Protection Commission should be more of a dialogue and education for the Ghanaian public and COVID-19 has made it possible for them to do that.

Computer Emergency Response Team (CERT-GH)

There was a slide presentation by Madam Audrey Mnisi Mireku, the CERT Lead at the NCSC. She elaborated on how an increase in fake news has been due to COVID-19, in addition to fraud, malicious attacks and many others. She again stated that due to COVID-19, children, the public, businesses, and the government experienced quite a number of challenges. She indicated that officers of the NCSC started working from home and configurations had to be made to allow remote access. She also stated that CERT-GH also received quite a number of incidents and requests for guidance to persons working from home in terms of how to assist them in keeping up with cybersecurity hygiene practices. She went ahead to share with the audience all incidents which were observed and were very prominent. She stated how there has been an increase in the impersonation of important personalities (VVIPs) in Ghana. Madam Mireku also made mention that even though most people were asked to work from home, the CERT team had to come to the office to work which made the CERT team frontline workers and therefore vulnerable. She concluded by sharing the Cybercrime/Cybersecurity Incident Reporting Points of Contact of the National Cyber Security Centre and pleaded with all to also share these contacts with their friends and others. She then urged everyone to be involved and not to be spectators, to help fight cybercrime in Ghana.

Ghana Armed Forces

There was a presentation made by Lt. Col. Elikem Fiamavle. He emphasised that cyberspace or domain has come to stay, and it is being recognised as the 5th domain of warfare. The Ghana Armed Forces also leverage some level of Communication and Information System for planning and decision making. He again stated that the Ghana Armed Forces Information Infrastructure and Systems are well protected and secured from cyber attacks. He elaborated on the key areas while indicating the common fraud experienced by the GAF which is recruitment fraud. He concluded his speech and stated that he was on standby for questions.

The moderator Mr. Clement Alabi of the NCSC, in his closing remarks noted that whilst Ghana had achieved key milestones in terms of cybersecurity development, the pandemic had exposed several weaknesses within our threat landscape, indicating that there was more work to be done.

WORKSHOP ON CYBERCRIME & ELECTRONIC EVIDENCE HANDLING FOR CRIMINAL JUSTICE SECTOR

The growth in the use and development of information and communications technologies go hand in hand with the rise of crimes committed against or through the use of computer systems. The Council of Europe's approach to protecting societies worldwide in cyberspace is based on the development and implementation of the Convention on Cybercrime (Budapest Convention), through a dedicated programme of capacity building for criminal justice authorities.

Sustainable Judicial Training programmes on cybercrime and electronic evidence have proved to be very effective in ensuring that judges, magistrates and prosecutors acquire and maintain sufficient knowledge to fulfil their roles effectively. The Council of Europe (CoE) has therefore developed an approach to Judicial Training aimed to empower countries to develop their own programmes of judicial training. This approach consists of providing the first level of training and then supporting countries as they integrate the available courses into their training curricula and the relevant Judicial Training strategies. As part of the programme of activities for the National Cyber Security Awareness Month 2020, the CoE, in collaboration with the National Cyber Security Centre (NCSC), organised a week-long Workshop on Cybercrime & Electronic Evidence Handling for the Criminal Justice Sector in Kumasi. The workshop was

held from October 19-23, 2020 at the Golden Bean Hotel, Kumasi.

This training was delivered by Ghanaian officials from judicial authorities, the department of public prosecution and law enforcement agencies, who shared knowledge and expertise with participants.

The workshop was attended by the Deputy Ashanti Regional Police Commander; DCOP Mr. David Agyemang Adjem, judicial authorities including justices of the High Court, District and Circuit Courts, prosecutors from the Ghana Police Service, officers from the Criminal Investigations Department (CID) and officers from law enforcement agencies including the Bureau of National Investigations (BNI) and the Economic and Organised Crime Office (EOCO).

Opening Remarks

DCOP Mr. David Agyemang ADJEM
Deputy Ashanti Regional Police Commander

DCOP Mr. David Agyemang Adjem welcomed all participants to the event stating that he was representing the Regional Commander. He expressed that lack of training is a weakness among law enforcement agencies, as it hinders the execution of duties. He also lauded the efforts of the Council of Europe and NCSC in organising the training programme. He advised all participants to adhere

to procedural correctness and protection of fundamental human rights in criminal investigations and prosecutions. He further encouraged trained officers to share their experience with colleague staff. DCOP Mr. David Agyemang Adjem thanked the organisers of the event and wished participants a successful training.

Remarks

Mr. Matteo LUCCHETTI
Programme Manager – Global Action on Cybercrime Extended (GLACY+)

Mr. Matteo Lucchetti explained that prosecutors and law enforcement agencies must have effective tools to prosecute. He explained that the training was aimed at enhancing the capacities of the judiciary and law enforcement agencies to actively tackle issues of cybercrime. He spoke on the ongoing collaboration with NCSC in strengthening capacities of the Ghanaian judiciary and law enforcement agencies based on the Budapest Convention. Mr. Lucchetti noted that Ghana collaborates with a number of states to uphold human rights and the provisions in the Budapest Convention. He noted that Ghana's efforts in cybersecurity have made it a hub for cybersecurity capacity building among Anglophone countries in West Africa. He wished participants fruitful deliberations and encouraged that participants share the knowledge learnt with fellow colleagues.

DAY ONE

On the first day, the trainers for the one-week capacity building programme introduced themselves. Dr. Gustav Yankson, the Director of the Cybercrime Unit of the Ghana Police CID and a CoE Trainer gave participants an overview of the week-long training and spoke on the role of the Cybercrime Unit of the Ghana Police CID. He also spoke extensively on the need for capacity building, especially for law enforcement agencies and the judiciary.

After the brief remarks, there was a short introduction around the table and participants introduced themselves and mentioned their expectations for the training. Participants were requested to fill a pre-event survey form in order to assess their understanding of the issues to be discussed. Mr. Lucchetti then took participants through a session on how to fill the pre-event survey forms.

Madam Hilda Mensah, a Child Online Protection Specialist with UNICEF Ghana delivered a presentation on behalf of the UNICEF Ghana Country Representative. In delivering her presentation, Madam Hilda Mensah thanked all participants for actively engaging in the workshop. She also thanked the NCSC and the CID for their deep collaboration with UNICEF Ghana in ensuring a robust cybersecurity ecosystem especially in the area of Child Online Protection (COP). Madam Mensah gave an overview of the activities children and young people engage in when online. She also

highlighted and discussed the risks and opportunities children face when exploring the internet. Madam Mensah also extensively discussed the role of the Criminal Justice Sector in ensuring a secure cybersecurity ecosystem especially in the area of COP. She also mentioned some of the initiatives that have been undertaken by UNICEF Ghana to scale up efforts in COP. These initiatives include the inauguration of the first Model Child Protection Digital Forensic Lab as well as the establishment of the first Child-Friendly Court; Circuit Court 5 at the Courthouse in Accra.

In her conclusion, Madam Mensah educated participants on the various PoC Channels and encouraged participants to report all cybercrime/cybersecurity incidents to the NCSC. The day's session ended at 5:00pm with Dr. Yankson introducing participants to the next day's training material.

DAY TWO

Dr. Yankson gave a recap of the previous day's activities. Mr. Zahid Jamil, a cybercrime and cybersecurity consultant for the Council of Europe gave an overview of global statistics relating to social media usage. He also spoke about the importance of international cooperation in the resolution of cybercrime. He stated that business e-mail compromises and ransomware form part of the top threats states and multinational corporations are exposed to. Mr. Jamil gave an overview of cybercrime and explained the nexus between technology, crime, a victim, an aid, a communication tool, a

storage medium and a witness.

He further gave an overview of the Budapest Convention and spoke on the three dimensions of the Convention, stating that the Convention serves as a standard, provides procedures for follow up and assessment and also serves for capacity building. Mr. Jamil also gave a brief history of the Budapest Convention. He also spoke on the various cybersecurity programmes being implemented by the Council of Europe. He took participants through the fundamentals of a cybercrime treaty and its functions as well as the benefits of a cybercrime treaty. In his conclusion, Mr. Jamil debunked some widespread rumours about the Budapest Convention. After a short break, the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako gave some brief remarks encouraging participants to actively engage in the week-long workshop. He also educated participants on the various achievements of the NCSC including the launch of the Safer Digital Ghana Campaign by H.E. Dr. Alhaji Mahamudu Bawumia. Before the day's session ended, Madam Jennifer Mensah introduced participants to some of the substantive laws in the Budapest Convention.

DAY THREE

Madam Jennifer Mensah gave a recap of what transpired the day before. She expanded on provisions covering international cooperation under the Budapest Convention and also explained provisions on mutual legal assistance.

Mr. Jacob Puplambu, the Head of Cybercrime Unit of the Economic and Organised Crime Office (EOCO) and a CoE Trainer, then gave a presentation on technology and internet basics. In his presentation, Mr. Puplambu highlighted the aim of the session and the reason for the training. He spoke extensively on computer parts and functions, and explained how virtual machines, computer systems and internet parts came to be. Mr. Puplambu also explained various network terminologies and expanded on connecting to the internet and the use of IP addresses. He also educated participants on surface web, deep web, and dark web.

Mr. Puplambu gave a thorough lecture on Business E-Mail Compromise, which has been identified as the most common international cybercrime. He explained the need to scrutinise evidence, educate employees and fellow staff and stay updated on customer information and habits. Dr. Yankson then took participants through a session on electronic evidence handling and introduction to computer forensics. He spoke on the use, types, characteristics, and sources of electronic evidence and also highlighted points on the processing of digital evidence through various provisions in the Electronic Transactions Act, 2008 (Act 772).

The day's session ended with Dr. Yankson presenting elaborately on sextortion and various elements that constitute the offence.

DAY FOUR

The fourth day of the training focused entirely on financial investigations and prosecutions. The trainer for this session was Justice Afia Serwaa Asare-Botwe. In her presentation, the learned judge explained the procedures to be followed when preparing a case for court. Her presentation also explained the importance of financial investigations and digital evidence in cyberspace. Justice Asare-Botwe further discussed the procedures to be followed in handling international digital evidence.

Participants were engaged in a series of case study exercises to ascertain their understanding of the training.

The day's session ended with a Q & A session to address various misconceptions and questions which the participants were facing.

Participants were later requested to fill a post-survey form, to enable the Council of Europe to properly assess their overall understanding of the modules taught within the one-week training.

After participants filled the post-survey forms, each participant shared with the team what they had learnt, and how they planned on sharing the knowledge with their colleagues. The day's session ended with a total recap of all that had ensued over the week.

Dr. Yankson, from the CID, congratulated participants for actively engaging in the five-day workshop. He further encouraged participants to conduct research to learn more about cybercrime and cybersecurity in order to aid them in the execution of their duties as judicial authorities and law enforcement agencies. The event which was a closed session saw the attendance of about 20 participants.

DAY FIVE

The final day's session focused on participants giving presentations on the various case studies they had solved. After being grouped into five teams, each team gave a presentation on the case solved and explained how they arrived at the solution. After all the teams gave their presentation, Dr. Yankson assessed their reports and lauded them for the good work done.

LAUNCH OF THE NATIONAL INFORMATION TECHNOLOGY AGENCY SECURITY OPERATIONS CENTRE (NITA SOC)



As part of the NCSAM 2020, the NCSC launched the Security Operations Centre (SOC) at the National Information Technology Agency (NITA) which will be responsible for monitoring and handling cyber-related incidents in the government sector including Ministries, Departments and Agencies (MDAs). The SOC is expected to compliment Ghana's efforts in building a resilient cyber ecosystem.

The attendees of the launch consisted of the Minister for Communications, Hon. Ursula Owusu-Ekuful, Chief Director of the Ministry of Communications, Madam Magdalene Apenteng, National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako, Acting Director-General of NITA, Mr. Richard Okyere-Fosu, NITA Board Chairman, Dr. Ezer Yeboah-Boateng, Board Members of NITA, the General Manager of

GDS Africa, the consultants in the operationalisation of the Security Operations Centre, Mr. Mohammed Zenuwah, chief directors, directors of IT of Ministries in Ghana, staff of NITA, staff of NCSC and guests.

Mr. Kwame Gyan, the moderator for the event introduced dignitaries present; Hon. Ursula Owusu-Ekuful, Minister for Communications, Hon. George Andah, Deputy Minister for Communications, Hon. Alexander Abban, Deputy Minister for Communications, Madam Magdalene Apenteng, Chief Director of MOC, Dr. Albert Antwi-Boasiako, National Cybersecurity Advisor, Dr. Ezer Yeboah-Boateng, Board Chairman for NITA, Mr. Richard Okyere-Fosu, Acting Director-General for NITA, Mr. Mohammed Zenuwah, General Manager of GDS Africa, Ing. Dr. Ken Ashigbey, CEO of Ghana Chamber of Telecommunications,

Mr. Selorm Adadevoh, CEO of MTN Ghana, Mr. Kofi Ofosu Nkansah, Managing Director of Accra Digital Centre and Mr. Kweku Kyei Ofori, Deputy Director-General of NITA. He then introduced Mr. Richard Okyere-Fosu, the Acting Director-General for NITA to give his welcome address.

Welcome Address

Mr. Richard OKYERE-FOSU
Acting Director General, NITA

Mr. Richard Okyere-Fosu, the Acting Director-General for NITA began by acknowledging the presence of the dignitaries and the guests. He stated that the event, the launch of the National Information Technology Agency Security Operations Centre



(NITA SOC), was a special occasion as it marked an important milestone in the delivery of NITA's mandate, which is mainly to regulate the provision of ICT, ensure provision of quality information communication, promote standards of efficiency and ensure high quality of service. He stated that the launch was a very significant step towards achieving the digitalisation agenda under the leadership of H.E. the President, Nana Addo Dankwa Akufo-Addo. He further acknowledged the great leadership direction NITA has had from the Hon. Minister, Mrs Ursula Owusu-Ekuful for achieving this and many other things NITA is pursuing. In conclusion, he expressed his gratitude to the World Bank for their support as well as to the vendors of the SOC and other institutions that helped achieve this project.

Opening Remarks

Dr. Albert ANTWI-BOASIAGO
National Cybersecurity Advisor

Dr. Albert Antwi-Boasiako, the National Cybersecurity Advisor, was called upon to give the opening remarks. He began by acknowledging the presence of the dignitaries and stated that the launch of the NITA SOC marked another milestone of the government's strategic invention to scale up Ghana's

cybersecurity readiness. He shared that the SOC establishment adds to similar inventions the government has implemented to improve Ghana's cybersecurity response across different sectors of the economy. The other establishments include the establishment of the Computer Emergency Response Team (CERT) at the National Communications Authority (NCA) and Bank of Ghana (BOG) Security Operations Centre (SOC). These interventions are critical elements for the operationalisation of the Cybersecurity/ Cybercrime Incident Reporting Points of Contact (POC).

He shared that the POC has impacted lives across the whole country, with more than 5000 citizens who have made contact with the National Cyber Security Centre (NCSC) through the National CERT from January to August 2020 to report incidents and also seek guidance and advisory in cyber-related issues. He congratulated NITA on the important achievement and stated that effective operationalisation of the SOC will significantly contribute to the work of the National CERT. Dr. Antwi-Boasiako expressed his appreciation to the staff of NCSC especially to the Director of Operations, Mr. Owusu Bediako-Poku and the Manager of Capacity Building and Awareness Creation, Madam Afia Darko Asante for their work in organising the National Cyber



Security Awareness Month (NCSAM) 2020 and particularly collaborating with NITA for the launch of the Security Operations Centre. He concluded by assuring the commitment of the officers of the NCSC to ensure the project delivers the best results to clients.

Remarks

Mr. Mohammed ZENUWAH
General Manager of GDS Africa



Mr. Mohammed Zenuwah, the General Manager of GDS Africa gave a brief remark acknowledging the company's French Partner, Intertek and also expressed their gratitude to the Ministry of Communications for the award of the contract that ensured the implementation of the NITA SOC.




the NITA SOC through the E- Government programme financed by the World Bank. He stated that NITA has acquired a SOC simulation and training platform that will equip and enhance the response capabilities of the SOC operators against any latest advanced cyber threats. He concluded by saying that the SOC, by ensuring information security and integrity, will reinforce the trust of the diverse national public and private stakeholders in the managed services provided by NITA and accelerate the digitisation of the Ghanaian economy.

Remarks

Dr. Ezer YEBOAH-BOATENG
The Board Chairman of NITA

Dr. Ezer Yeboah-Boateng, the Board Chairman of NITA commenced his remarks by acknowledging the presence of dignitaries. His opening remarks congratulated the Ministry of Communications for another remarkable feat by completing the implementation of

A photograph of Hon. Ursula Owusu-Ekuful, Minister for Communications, speaking at a microphone. She is wearing glasses and a patterned shawl. The background features a banner with the letters 'AJ' and 'CE' in blue, and a colorful circular logo on the right.

Keynote Address

Hon. Ursula Owusu-Ekuful

Minister for Communications

Hon. Ursula Owusu-Ekuful, Minister for Communications gave the keynote address and officially launched the NITA SOC. She began by stating that the presence of all guests there was a testament to the value they place on cybersecurity in the country and that it spoke of their support in the resolve to scale up cybersecurity development alongside the digitalisation efforts. She, on behalf of the President, H.E. Nana Addo Dankwa Akufo-Addo, officially welcomed everyone present to the launch as part of the celebration of the National Cyber Security Awareness Month (NCSAM) 2020. She remarked that as the Minister responsible for cybersecurity matters in government, she deems it a great honour to launch the NITA SOC infrastructure to improve the security of all the Ministries, Departments and Agencies (MDAs) and all the E-Government systems being put in

place. She stated that per analysis by the National CERT, malware-based attacks formed a great proportion of all cybersecurity incidents reported by Ministries, Departments and Agencies (MDAs). She also indicated government websites were subject to cyber-attacks including website defacements, Denial of Service (DoS) and Distributed Denial of Service (DDoS), among others. The SOC she added, will improve operational engagement and efficiency between the NITA SOC and the National CERT for effective response to cybersecurity incidents affecting MDAs. Hon. Ursula Owusu-Ekuful informed the gathering that the draft Cybersecurity Bill will be presented to parliament for passage into law before the session of parliament rises for the elections. She emphasised that it is critical that the country puts in place the legal and regulatory framework to facilitate responses to cybersecurity. The Cybersecurity

Bill is expected to improve Ghana's cyber protection. She stated that the NITA SOC will work with the National CERT and IT teams of the MDAs to ensure that all activities undertaken by the MDAs, within the digital ecosystem in the delivery of their official business are secured and safeguarded to ensure effective delivery of services by MDAs. She highlighted that one key benefit of the NITA SOC will be to improve security incident detection among MDAs to ensure a secure digital space in which they can operate and interact. In conclusion, she expressed her sincere appreciation to the project collaborators, NITA, NCSC, E-transform Project Consultant Team of the Ministry of Communications and the World Bank for funding the project under the e-transform project and project consultants of GDS Africa for delivering the project on schedule. She then officially launched the

National Information Technology Agency Security Operations Centre (NITA SOC).

Madam Magdalene Apenteng, the Chief Director of the Ministry of Communications gave the vote of thanks to close the event.

She thanked the Hon. Minister for Communications, Mrs. Ursula Owusu-Ekuful for her commitment to securing Ghana's Digital Journey, the members and Board Chair of NITA for their commitment in actualising the SOC, the staff of NCSC for collaborating with NITA and

MOC for facilitating this monumental stride. She then thanked guests for honouring the invitation and concluded by urging everyone to continue creating awareness and abiding by best cyber practices.

SESSION 2

Tour of the National Information Technology Agency Security Operations Centre (NITA SOC)

Hon. Ursula Owusu-Ekuful, Minister for Communications cut the ribbon and unveiled the plaque for the official launch of the NITA SOC. The ribbon cut was done in the presence of Madam Magdalene Apenteng, Chief Director, MOC, Dr. Albert Antwi-Boasiako, National

Cybersecurity Advisor, Mr. Richard Okyere-Fosu, Director-General, NITA, Dr. Ezer Yeboah-Boateng, Board Chairman, NITA and other dignitaries and heads of ministries, departments and agencies. The team from Intertek gave the delegation a walkthrough of the training facility

set up as part of the NITA SOC for the training of security analysts. Hon. Ursula Owusu-Ekuful stated this is a timely platform looking at the times we are in and hoped it will be put to optimum use.





WORKSHOP ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND RESILIENCE Part 2

The workshop was organised in collaboration with the MITRE Corporation under the Security Governance Initiative (SGI) to ensure the protection and resilience of critical infrastructure during and beyond the COVID-19 pandemic. The workshop sort to discuss the roles and responsibilities of designated Critical Information Infrastructure (CII) owners in ensuring the resiliency of their systems while raising awareness on the protection of critical infrastructure and essentials services. This was a virtual workshop.

The workshop was attended by stakeholders from key Government agencies, National Defence and Security and Information and Communications Technology providers. The meeting began with a brief introduction by the moderator of the session, Madam Jemima Owusu-Tweneboah. She outlined the schedule for the workshop which included remarks by MITRE, the National Cybersecurity Advisor and the Critical Information Infrastructure (CII) Lead of the NCSC. An opening remark was delivered by the National Cybersecurity Advisor. In his remarks he noted that the NCSC has not been active in engaging this sector, adding that CII contributes to the backbone of the economy. The Advisor went on to add that there was a need to plan to mitigate cyber attacks on the sector. He noted that the Government of Ghana has taken steps to ensure adequate law for the sector.

Additionally, audit and compliance laws are also being looked at by the NCSC and plans are underway to ensure CII owners are gazetted upon consultation. Inputs and perspectives about industry players were sought from stakeholders. The workshop he said was one of many ways to seek inputs in building a roadmap to guide the processes. Noting that the contributions of stakeholders are valued.

In delivering the remarks on behalf of MITRE, Madam Molly Schaefer stated that the group appreciated the effort of the NCSC and its leadership while indicating that the Security Governance Initiative has been ongoing for about 5 years and has seen significant cooperation between the two nations. She then went on to introduce her team which included Catherine Pertroll, Stacy Duhaney and Lauren Conroy.

It was reiterated that the mission of the initiative was to build cyber capacity in nations.

The Critical Information Infrastructure (CII) Lead of the National Cyber Security Centre Mr. Frederick Kwakye-Mafo added that there is a need for a cooperation. He touched on the Cybersecurity Bill being drafted and the need for the CII Directive. He shared that various African countries such as Cape Verde, Egypt and others have their own CII Directives. Adding that the directive seeks to operationalise the ETA sections 55 – 62 as it prescribes

minimum requirements for the registration of a CII. He also stated that there is a need to identify CII sectors for gazette and publication. Mr. Kwakye-Mafo informed the gathering that Ghana has identified 12 critical systems as its CII. These sectors include;

- ➔ National Defence and Security
- ➔ Banking & Finance
- ➔ ICT
- ➔ Energy
- ➔ Transportation
- ➔ Water
- ➔ Health
- ➔ Government Sector
- ➔ Emergency Services
- ➔ Food and Agriculture
- ➔ Manufacturing
- ➔ Mining

Adding that mining and manufacturing are the most recent sectors to have been added. He noted how GHACEM a manufacturing company has been pivotal in Ghana's development. Guidelines he stated are being developed in conjunction with the Assembly Press in Ghana. The Draft CII Directive is still undergoing considerations as stakeholders have been engaged to ensure easy buy-in when it is finally adopted.

Some of the functions of the directive include;

- ➔ Policy Adoption – have data protection concerns and clearly define people to be responsible for cybersecurity governance in all institutions.

➔ Technical & Organisations Measure – some of these include access controls, staff screening and cybersecurity awareness creation programmes.

➔ Monitoring for Crisis Alleviation – these include physical security, regular risk assessments, established audit regime, business continuity plans, backup plans, undergo cybersecurity exercises regularly to develop resilience and the adoption of relevant security best practises within the sector.

It was also discussed that incidents should be reported to sector CERTs with an established Point of Contact to liaise with the NCSC to manage incidents.

Some of the next steps discussed were the engagements with CII owners, registrations of CII handlers, development of risk framework and National Cyber Risk Assessment. Here, the MC went on to read out some questions that had been asked by the participants, some of which included;

- ➔ Timelines for the implementations of the CII Directive.
- ➔ Why education was not included in the critical systems identified.
- ➔ Why the Ghana Meteorological Agency (GMET) was not included.

It was stated that the CII Directive ought to be gazetted and that the education and GMET all fell under Government as outlined. He went on to add that sectors deemed critical could be reidentified if priorities changed.

Another participant inquired why it took so long for the government to identify critical information infrastructure. Here it was noted that an increase in digitalisation has ensured that attention is given to the sector looking at the potential risks posed. It was also inquired if the NCSC was adopting already existing security frameworks or forming new ones? Here the CII Lead stated that key stakeholders like the banks and telecommunications may have their own frameworks, however, the idea is to have a national standard framework that institutions comply with.

Presentation

Stacy Young DUHANEY

Ghana Cyber Critical Infrastructure Protection: Cyber CII protection is a key step in building a strong cybersecurity posture and identifying CII is a difficult process because different sectors are important to different people e.g fishing in Finland vs Alaska critical where as in Ghana it is and so there is the need to identify national goals as it helps the public understand what a nation values and ensure cooperation and collaborations. She further applauded the addition of mining and manufacturing. It is important to note responsibilities addressed in law in ensuring baseline protections for the reporting, response time identification of entity to report such incidents to and update reporting structure. She added that there is a need for CII regulators to know who is operating in the space for enhanced information sharing.

She gave an overview of the threat levels in Ghana which included routine cyber threats (fraud, ID theft, ransomware (malware on-demand being sold)). She credited the decrease in fraud to the work done by the NCSC, adding that organised crime that is cybercrime and cyber-enabled crime is another form of cyber-related crime identified in Ghana's ecosystem. Other threats are Insider crimes, resiliency issues and physical threats.

Other things to consider are;

- ➔ Broader national or institutional goals
- ➔ Degree of reliance on ICT in various sectors
- ➔ Threat environment
- ➔ Risk tolerance
- ➔ Existing cyber capabilities and resources

There is the need to assess risk in activity applicable to many aspects of the government work, accept the risk and consider your capabilities. Cyber risk management circle is not a one-time thing but a continuous circle.

She went on to explain that vulnerabilities are weaknesses that can be exploited and that not all weakness are technical. Vulnerabilities are potential flaws and someone with the technique to exploit that flaw as follows;

People – Process – Technology and Physical infrastructure. Cyber Risk is the intersection of value, threat and vulnerability. It was also noted that risk assessment is not concerned with immediate consequences, but recurrent examples as in elections, health and the like.

Critical infrastructure resiliency was also noted to be the use of resources to prepare for potential attacks and respond when something happens and limit the effects of the attack. Madam Duhaney ended the session and handed it over to Madam Lauren Conroy to take the participants through a series of practical sessions which comprised mostly of polls as a result of the virtual nature of the workshop. The practical session centred on the fictional state of Nion. Participants cooperated for a successful session.

A participant inquired if the MITRE Corporation has these sessions with private organisations and how much it costs. It was noted that with collaboration with the NCSC, the workshop could be replicated for other organisations at no cost. The NCSC team also noted that further training on the subject will be organised for stakeholders.

NATIONAL CYBER RISK ASSESSMENT (NCRA) WORKSHOP Part 2

The pandemic has led to rapid digital transformation globally which is of great importance to improve the functioning and efficiency of public and private organisations, as well as the well-being of populations. However, the growing threats and risks facing global cyberspace and digital networks, information systems and data can significantly reduce the expected benefits, and seriously harm the interests of Nations, their economies, institutions and people. In this regard, the National

Cyber Security Centre (NCSC), in collaboration with the United Kingdom (UK) Government, via the Commonwealth Cyber Programme and the UK's National Cyber Security Programme organised the National Cyber Risk Assessment (NCRA) Virtual Workshop to deliver cyber risk assessment training for Critical Information Infrastructure (CII) owners. The workshop was to help CII owners identify and assess the growing risks in cyberspace to critical information infrastructure. The event engaged representatives

from the Critical Information Infrastructure (CII) Sectors which included, Volta River Authority, Ghana Revenue Authority, Ghana Post, Ghana Gas, Ghana Civil Aviation Authority, Bank of Ghana, Ghana Stock Exchange, Ghana Water, National Petroleum Authority, Ghana Maritime and Tullow.

Welcome Address

Dr. Albert ANTWI-BOASIAGO
National Cybersecurity Advisor

In his opening remarks, Dr. Albert Antwi-Boasiako indicated that the workshop was a build-on for an earlier workshop that took place and as such stressed that the workshop was to build capacity to help deal with issues relating to Critical Information Infrastructure (CII). He also mentioned that the concept of the National Risk Assessment was introduced during a study visit to the United Kingdom (UK). In his submissions, he expressed appreciation to the UK Government for their support around CII Protection. To address the risks that Ghana faced, the National Cybersecurity Advisor indicated that there are multiple tools, processes that are used to

address risks. He stated that Ghana's cybersecurity development is in the formative stage and as such needed to take advantage and apply different methods and then choose the best one, or in some cases, customise our own methodology to address Ghana's risk associated with CII. He also added that the adoption will help Ghana understand its own infrastructure, the interdependency and vulnerabilities around CII, which will help in the categorisation of CII assets. Concluding his remarks, he indicated that information sharing constitutes an important element of the CII community and for that matter, CII owners need to interact and share information to address some gaps within the CII sector.

Remarks

Mr. Thomas HARTLEY
Deputy High Commissioner, UK
High Commission, Accra

Mr. Hartley began by expressing his pleasure to be part of the 2020 edition of the National Cyber Security Awareness Month celebration. He stated that COVID-19 has driven innovation very quickly, however, cybercriminals are using this current crisis as an opportunity to exploit weaknesses in cybersecurity. He further stated that cyber technologies in the wrong hands can be used to disrupt our lives and WannaCry in 2017 which affected 150 countries shows how real the cyber threats are. He stated that it is a constant battle with cyber criminals but the frontlines of cyber operations are in the Critical Information Infrastructure

companies and the key to success is working together. The collaboration between government, business and academia will reduce the threat faced from cyber criminals. He also added that the only responsible response is to build collective defences, and this was why workshops like the NCRA workshop are very important. Lessons learnt must be shared amongst all stakeholders to stand a chance of securing critical systems. He concluded by stating that the NCRA captures this learning and focuses on improving the cybersecurity of Critical National Infrastructure. He ended by stating that the UK Home Office was happy to share knowledge on NCRA but are also looking to learn from the experiences of the participants.

Overview of NCRA Process

Jeremy Ketteringham
ICT International Directorate,
UK Home Office

He began by welcoming all participants and outlined his background which is in Cybersecurity Capacity Building indicating that he has been delivering the National Cyber Risk Assessments for the past 3 years. He stated the process has been used successfully in over 300 organisations worldwide, including 4 African Commonwealth countries. The process is designed to hand over the tools, knowledge and skills to the local team. The objective is that at the end of the complete risk assessment process, the local team have all the skills and information required to carry out another risk assessment process on their own.

Cyber threats to Critical Information Infrastructure (CII) are growing in parallel to the digitisation of services. For nations to tackle this problem, there was the need for an understanding of the cyber risks to CII, to ensure effective mitigation. Understanding what infrastructure should be considered critical, what essential digital services exist, who owns them and where they sit within the overall priority view of a country's CII. The risk assessment is focused on estimating what the impact of a disruption will be to each of the services. There is a need to know how to defend against attacks but also how to respond when an attack occurs. The risk assessment begins with an interactive self-assessment survey to gather information about the threats, impacts and vulnerabilities of the systems that make up the CII. The Risk Assessment is a repeatable process to track how the risk is changing and how effective some of the measures have been, he said. Finally, he added that it is designed to analyse cyber risks using tools to visualise the national risk picture. The NCRA is built around a risk management cycle that Measures, Analyses, Prioritises and Acts. It identifies risk and mitigations which helps identify strategic investments and kickstarts cyber improvements. The NCRA will inform Ghana's National Cyber Security Strategy, assist in the development of Ghana's Cybersecurity investment programme by implementing strategic capacity building projects and create risk dashboards, measures and metrics to measure progress towards mitigation success. He concluded by highlighting various platforms and

capacity development programmes developed by the UK Home Office such as the Cyber Information Sharing Platform (CISP) which is a platform for organisations to share information about cybersecurity threats and also Cyber Essentials which is a simple and low-cost cybersecurity standard that many organisations who do not have the budget to gain high-end certifications can sign up for.

NCRA Questionnaire Walkthrough

Andrew CAMERON
ICT International Directorate,
UK Home Office

Mr. Cameron commenced his session by displaying the questionnaire and introducing the different sections of the questionnaire. These included the explanatory notes section which gives a detailed overview of the NCRA Questionnaire, the Organisation Questions section which gathers details about the organisation undertaking the assessment, the sector which they fall under, the critical systems in the organisation and the the prominence of cybersecurity within the organisation, the Systems 1-10 section which gathers information about the threats, impacts and risks pertaining to each system identified in the Organisation Questions and the Systems Summary section which captures all the information from the other sections into one to be analysed by the Data Analyst. Mr. Cameron then proceeded to fill out the questionnaire with data from a

fictitious company to demonstrate the information required for each section. He concluded by displaying the Systems Summary section to show how a completed questionnaire should look like.

Remarks

**Mr. Frederick
KWAKYE-MAAFO**
NCSC Critical Information
Infrastructure Protection Lead

Mr. Frederick Kwakye-Mafo began by thanking the UK Home Office team for the presentations. He then went ahead to give the participants and CII Owners assurance on information sharing. He highlighted the roles and persons responsible with regards to the NCRA process according to a Responsible, Accountable, Consulted and Informed (RACI) chart provided by the UK Home Office team while indicating that Hon. Ursula Owusu-Ekuful, Minister for Communications has been a champion for cybersecurity. The Head of the department role will be played by Dr. Albert Antwi-Boasiako, National Cybersecurity Advisor. The team lead for the engagement will be Mr. Frederick Kwakye-Mafo, the Critical Information Infrastructure Protection Lead. The organiser role will be Madam Audrey Mnisi Mireku, the Computer Emergency Response Team (CERT) Lead. The Cyber Expert role will be played by Madam Jemima Owusu-Tweneboah, a Cyber Analyst with the NCSC and the

Data Analyser role will be played by Mr. Gerald Awadzi, a Cyber Analyst. He continued to give assurance on how data received through the NCRA questionnaires will be stored and secured. He stated that the NCSC recognises the data collected is highly sensitive not only to the organisations in question but also to the country, so commensurate security measures have been put in place to protect it. He highlighted the existence of a secure portal for the exchange of such confidential information, which is the Trusted Information Sharing Network (TISN). The CII Owners will have to register to have access to the TISN. The TISN will also facilitate the training and capacity building of the CII Owners. He concluded by requesting questions from the participants.



Mr. Eric Asamoah, one of the participants, asked how soon CII organisations will begin to share these vulnerabilities and attacks, if any, with the NCSC and what protocols have been put in place for accessing the secured portal. Mr. Kwakye-Mafo answered the questions by giving details of the security mechanisms put in place for the TISN. He also walked through the various processes that have to take place prior to officially engaging the CII Owners.

Madam Jemima Owusu-Tweneboah concluded the workshop by expressing gratitude to all the participants for honouring the invitation, giving special thanks to the UK Home Office team for the knowledge transfer. She finally requested the participants send an email with their contact information and the institution they represented to info@cybersecurity.gov.gh to foster further communication.

WORKSHOP ON LESSONS LEARNT BY THE TELECOMMUNICATIONS SECTOR DURING COVID-19 CRISIS

The National Cybersecurity Centre (NCSC) together with the National Communications Authority, and the Telecommunications Service Providers held a virtual workshop to discuss the impact of the COVID-19 pandemic on their operations and lessons they learnt within the period of the pandemic. The workshop began with a welcome address from Mr. Prince Sefa, the Deputy Director-General of the NCA. The NCA noted that it provided the Service Providers with security passes to enable them to commute easily during the lockdown period with a total of 3, 672 passes being distributed. The NCA also provided support to consumers by providing dedicated lines of contact and online platforms for reporting challenges with service providers. The meeting had a representation from AirtelTigo, Glo, MTN, Vodafone, National Communications Authority CERT, National Cyber Security Centre, Africa Online, Comsys, amongst others.

Welcome Address

Mr. Prince SEFA

Deputy Director-General, National Communications Authority

In his opening address, Mr. Prince Sefa welcomed all participants to the workshop and proceeded to state some support the NCA rendered to the Service providers during the

COVID-19 pandemic lockdown. He spoke on the extra spectrum given to some service providers to ensure that users of telecom networks were provided with a quality network usage experience. He explained that this spectrum was given at no cost and this was to ease the congestion which resulted from the surge in data usage by subscribers. Due to this, during and post COVID-19 lockdown, the NCA-CERT noticed a rise in threats and vulnerabilities which was because of users making more use of the internet. He added that the NCA supported the Ghana Health Service in contact tracing as the Authority's position as the telecom regulator was required for the collection of passive data logs from the operators. The Authority also assisted in publishing and publicising contact details for COVID-19 related enquiries. The NCA engaged the constituents via virtual meetings which were held almost daily and created WhatsApp platforms to receive real-time complaints that required expeditious response.

He explained that the pandemic has given the Authority more insight into its operations. This has taught the Authority to:

➔ Keep open-door policies with service providers as many operational challenges that confronted the service providers were noticed.

➔ Continuously interact with the service providers on issues of fibre cuts incidents as it is one of the most reported incidents.

➔ Use technological means of communicating with its constituents.

He explained that, after the lockdown, some service providers were invited to the NCA-CERT to appreciate the Authority's cybersecurity consciousness. He explained that the Authority has planned to keep a robust line of communication with service providers and be open to the change the industry is noted for. He expressed gratitude to all participants and wished all a fruitful workshop.

Presentation

Mrs. Jennifer MENSAH

NCA-CERT

Mrs. Jennifer Mensah, starting her presentation, expressed gratitude and stated that her presentation will cover the legal aspect of cybersecurity. She presented on the cybersecurity obligations; data protection conferred by law which the service providers are to comply with. She continued that, with the outbreak of the pandemic, there had been an increase in cyber-attacks at an alarming rate exploiting the fear and uncertainty of individuals,

caused by the unstable social and economic situation. She gave a statistic by the UNICEF which stated that children are at an increased risk of harm online as a result of the pandemic. She noted that essence of cybersecurity and data privacy compliance is important in this COVID-19 world of today.

She stated that the NCA has laws and regulations that it operates with and one of these is the Electronic Communications Regulations and this confers cybersecurity obligations on service providers to protect the service they offer, network and messages sent across the network. She explained that it is important that these laws and regulations are complied with and also, it is the expectation of the NCA that, in complying with the regulations, service providers will have cybersecurity governance and risk maintenance frameworks and relevant technical controls should be put in place to reduce vulnerabilities and also, develop measures of complying with organisational cybersecurity policies.

Regarding reports sent by the NCA-CERT, Mrs. Jennifer Mensah stated that it is important service providers collaborate with the CERT in resolving incidents. Speaking on the Regulations (5), she explained that, the law mandates service providers to inform users of risks they notice on their network and measures of mitigating these risks. Service providers need to ensure the privacy of users by putting in place best practices to ensure that subscribers are protected. She made it known

that, due to these laws, the NCA has now instituted in the Authorization and license, the obligation to ensure privacy as there was none previously. Technical and organisational measures, Information security management and cybersecurity awareness programmes for both organisations' staff and subscribers are some initiatives the NCA is expect service providers to implement in their organisations.

Speaking on Data Protection, Mrs. Jennifer Mensah noted the importance of registering with the Data Protection Commission, as it is mandated by law. She expressed the need to have a Data Protection Supervisor certified by the Commission, as the supervisor will be responsible for supporting the organisation in complying with the Data Protection Act. Mrs. Jennifer Mensah explained, in complying with these regulations and laws, it is important to cooperate with law enforcement bodies by providing them with appropriate information if the need arises.

Presentation

Mr. Spilker WIREDU
NCA-CERT

Mr. Spilker Wiredu presented lessons learnt by the NCA-CERT during the COVID-19 period. He stated that on a daily basis, the NCA-CERT receives intelligence reports from the CERT-GH. These reports are analysed by the CERT and forwarded

to respective constituents. He also mentioned that these reports are compared to global statistics to know if the data correlates and further research is carried out. He added that the NCA-CERT is currently in partnership with Japan CERT (JP CERT). The NCA-CERT has a probe in its network which gives more insight into the JP CERT network with the help of their honeypots situated all around, collating information on attacks occurring in the world. He also mentioned some incidents the NCA-CERT has resolved as a result of this partnership. Mr. Spilker Wiredu shared statistics of vulnerabilities' trends both locally and globally.

Presentation

Ms. Jacqueline
HANSON KOTEI
MTN Ghana

Ms. Jacqueline noted that her presentation covered lessons learnt before, during and after COVID-19. She mentioned that MTN Ghana anticipated new trends in cybersecurity threats before the outbreak of COVID-19. Noting that before COVID-19, MTN had a well-planned high-level strategy that involved strengthening their information security team's capability to enable secure and innovative corporations, collaboration with key partners to promote resilience and reduce incident severity of cybersecurity breaches and regulate third party activities within the company environment.

During COVID-19, about 87% of the staff of the company were asked to work from home. Due to the surge in online activities, there was an increase in malware activity that originated from user accounts and also an increase in phishing attacks against front liners particularly. Increased VPN accesses and increased capacity of the help desk as they were also working from home. Due to the business continuity plans developed, there was a seamless transition of work operations during the lockdown era. There were engagements with the NCA, Ministry of Communications (MOC) and other organisations. She added that about 46% of staff were still telecommuting. Ms. Jacqueline Hanson Kotei noted that cybersecurity tips were developed and shared with staff on their platforms. There have been awareness programmes that involved high-risk users, the technical team and the entire company. There was a new development of a chatroom involving the CEO, CTO, and all staff where security questions are raised and answered. Post COVID-19, MTN has strategised some business continuity plans for a continuous operation. These include training annually to equip technical staff, training for local CERT and operationalising it, education and awareness across the whole organisation and also strengthening the governance of work-from-home policy amongst others which have been put in place for business continuity. MTN has considered undertaking cyber exercises, cyber threat tools, training of responders and frequent cyber-attack simulations for staff to equip them.

Presentation

Mr. Raymond FOLLEY
COMSYS

Beginning his presentation, Mr. Folley noted that the company developed a business continuity plan. Therefore, with the COVID-19 pandemic, this plan was leveraged to ensure operations continued seamlessly. He mentioned that about 80% of staff had to work from home as a result of the pandemic. Staff were securely connected via VPNs for operations. During the pandemic, customer support was remotely done therefore, clients of the company were given unique accounts that worked with them in responding to their complaints. About 20% of staff worked in the office, therefore all COVID-19 protocols were implemented to prevent the spread of the virus and there was an improvement in physical security to protect staff on site.

Mr. Folley noted that Comsys needed to build more capacity and awareness therefore, training was organised to bring staff up to speed. Challenges of staff were also factored into the capacity building programme. Due to the work from home policy, clients and Comsys staff encountered challenges of having to work with a non-IT staff of clients. Mr. Folley explained that internet traffic had to be moved to clients' homes for their work operations. Going forward, Comsys will include non-IT personnel for all technical training to equip them with basic knowledge of IT. Additionally, the network will be dynamic and not static to enable traffic to be moved easily.

Presentation

Mrs. Audrey Mnisi MIREKU
National Cyber Security Centre (NCSC)

Mrs. Mireku stated that there is an ongoing project where information will be shared on vulnerabilities, incidents and reports gathered in the telecom ecosystem amongst constituents. She added that the Ministry of Communications has come up with an initiative of developing a platform for sharing this information gathered from constituents.

The National Cyber Security Centre, through the Ministry of Communications, has planned to engage with all the telecommunications industry stakeholders to collate their requirements for developing the platform. The platform will include;

- ➔ A user-friendly interface
- ➔ End-to-end encryption that is ensuring confidentiality, integrity and availability
- ➔ Availability both offline and online
- ➔ Sanitised data to be shared with other stakeholders
- ➔ Subscribe and unsubscribe options

With these, Mrs. Mireku encouraged the constituents to share with NCSC their suggestions on the initiative.

Other Matters

Concerns were raised on whether the NCA has plans of organising a forum for all constituents to properly educate them on these laws and regulations as some of these service providers are not well inclined with these laws. The NCA responded that plans are being made towards this initiative and constituents will be reached out to as soon as objectives for the forum are finalised.

Concerns were raised on whether there were programmes or measures that address cyber fraud perpetrators that install schemas on ATM machines and as a result, clone peoples' data on ATM cards. Comsys noted that the company does not manage that aspect of the ATM operations, however, they encourage financial institutions to ensure maximum security at the ATMs. Currently, there is not a concrete solution that monitors these acts but there are cameras at every ATM that monitors user activities.

It was inquired that with other sectors also having sectoral CERTs, how did this stakeholder engagement align with the development that needs to continue the operations entrenched

at the sectoral CERTs. Mrs. Mireku noted that this initiative is a way of reinforcing the activities of the CERTs and does not take away their mandates. This is to provide a centralised platform for gathering intelligence of activities happening in the telecom ecosystem. Giving the final remarks, the chairman - Mr. Prince Sefa expressed his gratitude to all staff from the National Communications Authority and the National Cyber Security Centre, Mobile Network Operators, Internet Service Providers and Broadband Wireless Access providers and all distinguished participants. for a fruitful discussion. He also encouraged all participants to be mindful in enforcing COVID-19 protocols in order to be safe. He encouraged all to telecommute if possible, to ensure COVID-19 protocols are enforced in workplaces. The workshop saw the participation of about 30 participants.

WORKSHOP ON CYBERCRIME & ELECTRONIC EVIDENCE HANDLING FOR CRIMINAL JUSTICE SECTOR

The growth in the use and development of information and communications technologies go hand in hand with the rise of crimes committed against or through the use of computer systems. The Council of Europe's approach to protecting societies worldwide in cyberspace is based on the development and implementation of the Convention on Cybercrime (Budapest Convention), through a dedicated programme of capacity building for criminal justice authorities.

In line with this, sustainable Judicial Training programmes on cybercrime and electronic evidence handling have proved to be very effective in ensuring that judges, magistrates and prosecutors acquire and maintain sufficient knowledge to fulfil their roles effectively. The Council of Europe (CoE) has therefore developed an approach to Judicial Training aimed to empower countries to develop their own programmes of judicial training. This approach consists of providing the first level of training and then supporting countries as they integrate the available courses into the training curricula and the relevant Judicial Training strategies. As part of the programme of activities for the National Cyber Security Awareness Month 2020, the CoE in collaboration with the National Cyber Security Centre (NCSC), organised a week-long Workshop on Cybercrime &

Electronic Evidence Handling for Criminal Justice Sector in Accra. The workshop was held from October 26 - 30, 2020 at the Alisa Hotel, Accra.

This training was delivered by Ghanaian officials from Judicial Service of Ghana the department of public prosecution and law enforcement agencies, who shared knowledge and expertise with participants.

The meeting was attended by officials of the Criminal Justice Sector including officials from the Criminal Investigations Department (CID) of the Ghana Police Service, the Attorney General's Department, Bureau of National Investigations (BNI), Economic and Organised Crime Office (EOCO) and the Narcotics Control Commission.

Welcome Address

Matteo LUCCHETTI

Programme Manager – Global Action on Cybercrime Extended (GLACY+)

Mr. Lucchetti lauded the Honourable Minister for Communications for the good work being done especially in the area of cybersecurity, adding that the steps being taken by the Government to operationalise cybersecurity, including the formation of the National Cyber Security Technical Working Group (NCSTWG) and the establishment of the Cybercrime/Cybersecurity

Incident Reporting Points of Contact (PoC) were laudable. He commended Ghana for becoming a hub for cybersecurity capacity building in West Africa. He finally thanked participants for joining the workshop and urged them to engage actively in the sessions.

Remarks

Madam Hilda MENSAH

Child Protection Specialist UNICEF Ghana

Madam Hilda Mensah, a Child Protection Specialist with UNICEF Ghana delivered a presentation on behalf of the UNICEF Country Representative. In delivering her presentation, Madam Hilda Mensah thanked all participants for actively engaging in the workshop. She also thanked the NCSC and the CID for their deep collaboration with UNICEF in ensuring a robust cybersecurity ecosystem in Ghana especially in the area of Child Online Protection (COP). Madam Mensah gave an overview of the activities children and young people engage in when online. She also highlighted and discussed the risks and opportunities children face when exploring the internet. Madam Mensah also discussed extensively the role of the Criminal Justice Sector in ensuring a pristine cybersecurity ecosystem especially in the area of COP. She then mentioned some of the initiatives

that have been undertaken by UNICEF to scale up efforts in COP. These initiatives include the inauguration of the First Model Child Protection Digital Forensic Lab as well as the establishment of the first Child-Friendly Court; Circuit Court 5 at the Courthouse Accra.

In her conclusion, Madam Mensah educated participants on the various PoC Channels and encouraged participants to report all cybercrime/cybersecurity incidents to the NCSC.

Remarks

Dr. Albert ANTWI-BOASIAGO
National Cybersecurity Advisor

In his remarks, the National Cybersecurity Advisor thanked all participants for participating in the workshop and admonished the general public to scale up their personal cybersecurity efforts. He highlighted key milestones achieved by the Government in the area of cybersecurity including the ratification of the Convention on Cybercrime (Budapest Convention) and the African Union Convention on Cybersecurity and Personal Data (Malabo Convention), the establishment of the PoC and the deployment of capacity building programmes for the Criminal Justice Sector. He noted that a lot of work had been done especially in the area of Child Online Protection (COP) including the inauguration of the First Model Child Protection Digital Forensics Lab, which was through the joint effort of UNICEF, the CID and the NCSC. He also noted the launch of the Child Online Protection Reporting Portal by the NCSC

earlier in the month of October. Dr. Antwi-Boasiako encouraged all participants to report all cybercrime/cybersecurity incidents to the NCSC via the PoC to aid in the overall development of Ghana's cybersecurity.

DAY ONE

Dr. Herbert Gustav Yankson, the Director of the Cybercrime Unit of the Ghana Police CID and a CoE Trainer took participants through the course objectives and course outline. After the brief introduction by Dr. Yankson, Mr. Lucchetti took participants through the pre-event survey forms shared to enable them to complete the forms appropriately to aid the CoE in their research and analysis.

Dr. Yankson then gave a presentation on gender-based violence in cyberspace and elaborated on the concept of gender-based violence and the challenges to investigations and prosecutions. He also threw more light on cyber violence and gave some examples of cyber violence to include malicious text messages, child pornography, cyberstalking, offensive speech, online grooming. He also spoke extensively on the violation of privacy and its effect on the overall cybersecurity of a country.

DAY TWO

Mr. Branko Stamenkovic, a Deputy Public Prosecutor of the Republic of Serbia and a CoE Trainer gave a brief

presentation. He gave an overview of Serbia's civil proceedings, speaking on cybercrimes and cybercriminals as well as the position of civil law countries on criminal proceedings. Moving further into the topic of cybercrime, he noted that the purpose of the training was to expose participants to the world of cybercrime. He took the participants through what cybercrime is and entails, the Budapest Convention, International Organisations of cybercrime, cybercrimes and case studies, and the concepts of cybercrime that are considered types of crime under most legislations and international standards.

He further explained some cyber-related concepts such as skimming, botnets, and cyber warfare, where he referred to 2017 as one of the years that recorded some significant ransomware attacks. He also explained the diverse nature of cybercrimes, which include technology aiding the crime or it is the victim of a crime and even technology as the communication tool for the perpetuation of the crime.

Speaking on the Budapest Convention, he discussed the Convention's scope, coverage, additional protocol and what it means to join the Convention. He presented on related International Organisations: the United Nations (UN), the African Union (AU), the International Criminal Police Organisation (INTERPOL), Pacific Islands Law Officers' Network (PILON), and Council of Europe. He highlighted their background, inception, functions and some initiatives that have been taken.

After the coffee break, Madam Jennifer Mensah a deputy director at the Computer Emergency Response Team of the National Communications Authority and a CoE Trainer presented on the Substantive and Procedural laws of the Budapest Convention. The aim of the presentation, she noted, was to provide the participants with a comprehensive understanding of the offences against the confidentiality, integrity and availability of computer systems and data established in accordance with the Budapest Convention. She went through some need-to-know terms, which include traffic data, service provider and computer system. She also identified for the participants, parts or sections of various Ghanaian laws that imbibe and reflect the Budapest Convention. Some of these laws include the Electronic Transactions Act, 2008 (Act 772) and the Copyright Act, 2005 (Act 690). Madam Mensah explained the 'Going Dark Phenomenon' which refers to the phenomenon by which government agencies have a legal right to access particular communications but lack the technical ability to do so, often because technology companies have deployed strong encryption to shield the information and how it serves both the good and the bad. For the final phase of her presentation, she looked into the legal aspects of international cooperation, such as mutual legal assistance and voluntary cooperation.

DAY THREE

Mr. Jacob Puplampu, the Head of the Cybercrime Unit of the Economic and Organised Crime Office (EOCO) and a CoE Trainer gave a presentation on computer and internet basics. He took participants through the various components, parts and functions of computer systems. He focused on computer hardware and software, explaining how they operate and their importance to cybersecurity, as well as how cybercriminals use these computers to carry out cybercrime. He explained the deep web and dark web, emphasising their differences and the nature of the dark web.

Dr. Yankson gave a presentation that encompassed law enforcement, electronic evidence, processes and requirements in the gathering and handling of evidence and the errors law enforcement officers make that affect the quality of evidence gathered. He also explained the territorial scope of offences under the Electronic Transactions Act, 2008 (Act 772). Some of the sections under the Act he addressed included Sections 100, 102 and 106 of Act 772. In discussing evidence collection, he spoke on search sites basic rules and documenting the scene. He spoke on the Association of Chief Police Officers (ACPO) principles of digital-based evidence.

DAY FOUR

Mr. Puplampu gave a quick recap of the week's activities and highlighted salient discussion points that had been elaborated. This was followed by a presentation by Justice Afia Serwaa Asare-Botwe. In her presentation, Justice Asare-Botwe expanded on financial investigations, prosecutions and applications. She noted, the discussion was to touch on why financial investigations require a certain approach; how to investigate; legal terms related to financial crimes; skills as financial investigators; understanding the different legal frameworks and how financial investigators are to understand their own laws and regulations.

Some additional topics she spoke on were what financial crimes are, offences involving dishonesty and cyber-related crimes (sextortion, terrorist financing, sim box fraud and money laundering). While presenting, she touched on judicial response to these new cybercrimes and gave some tips on how to prepare for a court case. For these discussions, she referred to Act 772 and Anti Money Laundering (Amended) Act, 2014 (Act 874) as well as some cases such as the Bernie Madoff case (financial crime) and the Cubagee case named Cubagee vs. Asare and others (NO. J6/04/2017) [2018] where she discussed discretions and considerations. In

discussing evidence from abroad, she spoke on applicable rules, integrity, admissibility and legality. She also discussed measures of privacy and proportionality.

Mr. Stamenkovic from the CoE also took the participants through a series of team-building exercises for revision to assess and observe the application of principles learnt by participants during the week-long workshop. The assignment was to be done by participants in teams, as he had explained, and a presentation was to be made by each team the next day.

DAY FIVE

Dr. Yankson gave a presentation on advanced search techniques for Open-Source Intelligence (OSNIT) and Social Media Intelligence (SOCMINT). He explained what these two disciplines are, what they involve, and their importance. He further explained how they could be utilised by law enforcement.

Each team, through an elected team leader, was then invited to present findings and results on the tasks assigned on the previous day. The tasks had case scenarios that

required the teams to make use of all the information and knowledge gathered through the presentations that had been made by the CoE Trainers. Some of the case studies were on the WannaCry ransomware which affected most systems in 2017.

The week-long workshop ended with some closing remarks from Dr. Herbert Gustav Yankson, who encouraged participants to share the knowledge learnt with fellow colleagues in order to build the capacity of the criminal justice sector especially in the area of cybersecurity. He also urged participants to conduct personal research into the area and take advantage of all opportunities to learn more about cybercrime/cybersecurity. This workshop also saw the participation of about 25 participants.

REGIONAL CAPACITY BUILDING AND SENSITISATION EXERCISE

Following the official launch of the NCSAM 2020, a series of regional sensitisation activities were conducted parallel to the weekly high-level events organised in Accra.

The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako led a team of officers from the National Cyber Security Centre and a representative from the Ministry of Communications on this nationwide exercise to account to the public on what the Government through the NCSC/MoC has achieved over the past three and half years. This engagement comprised direct engagements (under strict compliance with COVID-19 protocols) with key stakeholder groups in the regions (trade, professional bodies, civil society groups, etc.) and media engagement via selected media outlets (television and radio) nationwide.

Due to the pandemic which resulted in the temporary closure of schools nationwide, the schools' sensitisation which underpins the regional activities did not happen. Volta and Oti regions were not visited due to circumstances related to security complications at the time in the regions.

A total of 1,235 participants were reached out to for the workshop engagements and the media outreach targeted at citizens within the particular region. The workshops were attended by Regional Ministers, Members of Parliament, Directors & Deputy Directors of Regional Coordinating Councils, Heads of Public & Private Institutions, Regional Ghana Journalists Association Chairmen, Journalists, Regional Security Commanders, Managers and Officers of selected government institutions.

Highlights of Activities

Upper West Region

The nationwide sensitisation programme began on October 3, 2020 in Wa. The workshop in this region took place at the Ghana National Association of Teachers



(GNAT) Hall with 94 participants drawn from 10 districts. The exercise was facilitated by Mr. Aaron Felix Opoku Boateng, a Programmes Officer for the Capacity Building and Awareness Creation Unit of the NCSC.

Participants were engaged in the Government's key achievements in Ghana's Journey towards the development of cybersecurity and were also educated on cyber hygiene best practices.

Upper East Region



Upper East regional activities took place in the regional capital, Bolgatanga on October 6, 2020. The National Cybersecurity Advisor had a media engagement at Tanga Radio and A1 radio. Following the media engagement, a two-hour workshop was organised for the Regional



Coordinating Council and members of the Ghana Journalists' Association with 60 and 25 participants representing, respectively.



The two workshops which were organised separately at the premises of the Regional Coordinating Council was facilitated by the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako. The RCC engagement drew participants from institutions such as the Ministry of Gender, Children and Social Protection, National Disaster Management Organisation (NADMO), among others.



Northern Region



Activities in the Northern region were held in Tamale on October 7, 2020. The National Cybersecurity Advisor had a 15-minute interview session each on Savannah Radio and Zaa Radio. Two workshops were organised for the Regional Coordinating Council and members of the Ghana Journalists' Association with 45 and 42 participants representing, respectively. The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako facilitated the workshops.



Savannah Region

The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako educated the people of Damago and its surrounding towns during an hour-long media interview on Pad FM. Capacity Building and Sensitisation exercise in this region involved 105 participants drawn from the Regional Coordinating Council and Nation Builders



Corps (NABCO). The event was graced by the Regional Director of the Coordinating Council, Regional Police Commander, Regional NABCO Coordinator, among others. The National Cybersecurity Advisor, Dr. Albert Antwi- Boasiako facilitated the workshop. The team was in the region on October 8, 2020.



North East Region

Activities in the North East region took place in the regional capital Nalerigu on October 9, 2020. The team led by the Communications Officer of the NCSC, Madam Esther Ohenewaa Brown had a one-hour media engagement at Tizaa FM. Following the media engagement, a two-hour workshop was organised for the Regional Coordinating Council.

The workshop which was held at the premises of the Regional Coordinating Council was facilitated by Mr. Aaron Felix Opoku Boateng. The exercise which recorded 50 participants witnessed the participation of

the Regional Minister, Hon. Solomon Boar, the Regional Police Commander, the Regional Coordinating Council Director, Regional NADMO Coordinator and other regional security representatives.



Eastern Region



Activities in the Eastern region took place in the regional capital Koforidua on October 13, 2020. A two-hour workshop was organised for institutions under

the Regional Coordinating Council and members of the Ghana Journalists' Association with 50 and 35 participants representing, respectively.

The two workshops which were organised separately at the premises of the Regional Coordinating Council was facilitated by the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako. Participants were drawn from institutions such as the Ministry of Gender, Children and Social Protection, National Disaster Management Organisation (NADMO), Fire Service, Immigration, Ghana Police Service, among others. The National Cybersecurity Advisor also had a one-hour media interview at Taste FM.



The two workshops were separately held in Cape Coast on October 14, 2020 at the premises of the Regional Coordinating Council and Pempamsie Hotel respectively and were facilitated by the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako. The team, led by the Communications Officer, had a media engagement at Eagle FM and ATL FM.



On October 17, 2020, the team also organised a Youth Engagement on Cybercrime and Cybersecurity for the youth of Awutu Senya West Constituency. The event which was facilitated by the National Cybersecurity Advisor witnessed the participation of 110 youth including the Member of Parliament for the Constituency and Deputy Minister for Communications, Hon. George Andah.

Central Region

The Capacity Building and Sensitisation exercise in this region involved 75 participants drawn from institutions under the Regional Coordinating Council and 20 participants from the Rotary Club of Cape Coast-Central.



Western Region



Activities in the Western region were held in Takoradi on October 15, 2020. The National Cybersecurity Advisor had interview sessions on Sky Power FM and Fox FM. Two

workshops were separately organised for institutions under the Regional Coordinating Council and members of the Ghana National Association of Teachers (GNAT) at the premises of the Coordinating Council and GNAT Hall, respectively. A total of 131 participants represented comprising 87 RCC members and 44 GNAT members.



The National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako facilitated the Coordinating Council session and Mr. Aaron Felix Opoku Boateng served as the facilitator for the GNAT exercise.



On October 17, 2020, the team also organised a Youth Engagement on Cybercrime and Cybersecurity for the youth of Ahanta-West Constituency where 74 participants represented. The event which was facilitated by the National Cybersecurity Advisor involved the Member of Parliament for Ahanta-West Constituency, Hon. Ebenezer Kojo Kum. The National Cybersecurity Advisor also had a media interview on Ogya FM.

Western North Region



The Western North regional activities took place in Sefwi-Wiaso and Sefwi-Juaboso on October 16, 2020. The team led by the Communications Officer of the NCSC had a media engagement at De-Beat FM and Radio Rainbow to sensitise the general public on the government's achievements and cyber hygiene best practices. During a phone session, Mobile Money (MoMo) fraud was the key issue raised by listeners.

Ashanti Region



The Ashanti regional activities took place in Kumasi on October 20, 2020. The National Cybersecurity Advisor had a media engagement at Adeshye FM. Following the media engagement, a two-hour workshop was organised for staff of the Regional Coordinating Council and members of the Ghana Journalists' Association.

The two workshops which were organised separately at the premises of the Regional Coordinating Council was facilitated by the National Cybersecurity Advisor, Dr. Albert Antwi-Boasiako. It recorded about 130 participants comprising 85 RCC members and 45 GJA members.

Bono Region



The Bono regional activities took place in Sunyani on October 22, 2020. The team, led by the Communications Officer of the NCSC, had a media engagement at Ark FM. Following the media engagement, a two-hour workshop was organised for the Regional Coordinating Council and members of the Ghana Journalists Association.

The two workshops which were organised separately at the premises of the Regional Coordinating Council was facilitated by Mr. Aaron Felix Opoku Boateng and Mr. Isaac Socrates Mensah, a Triage Officer with the Computer Emergency Response Team (CERT) of the NCSC. The exercise recorded 105 participants comprising 45 representatives from the RCC and 60 representatives from the GJA.



Bono East Region



Activities in the Bono East region were held in Techiman on October 23, 2020. The team had an interview session on Classic FM.

Following the media interview, a capacity building workshop was held at the premises of Regional Coordinating Council. The exercise witnessed the participation of the Regional Minister, Hon. Kofi Amoakohene, the Regional Coordinating Council Director, Heads of Public Institutions, Security Personnel, among others. A total of 40 participants were involved in the exercise.

Ahafo Region

The Ahafo regional activities took place in the Regional capital, Goaso, on October 24, 2020. The team had a media engagement at Success FM to sensitise the general public on the government's achievements and cyber hygiene best practices.

During a phone session, MoMo fraud and online scam were the key issues raised by listeners.

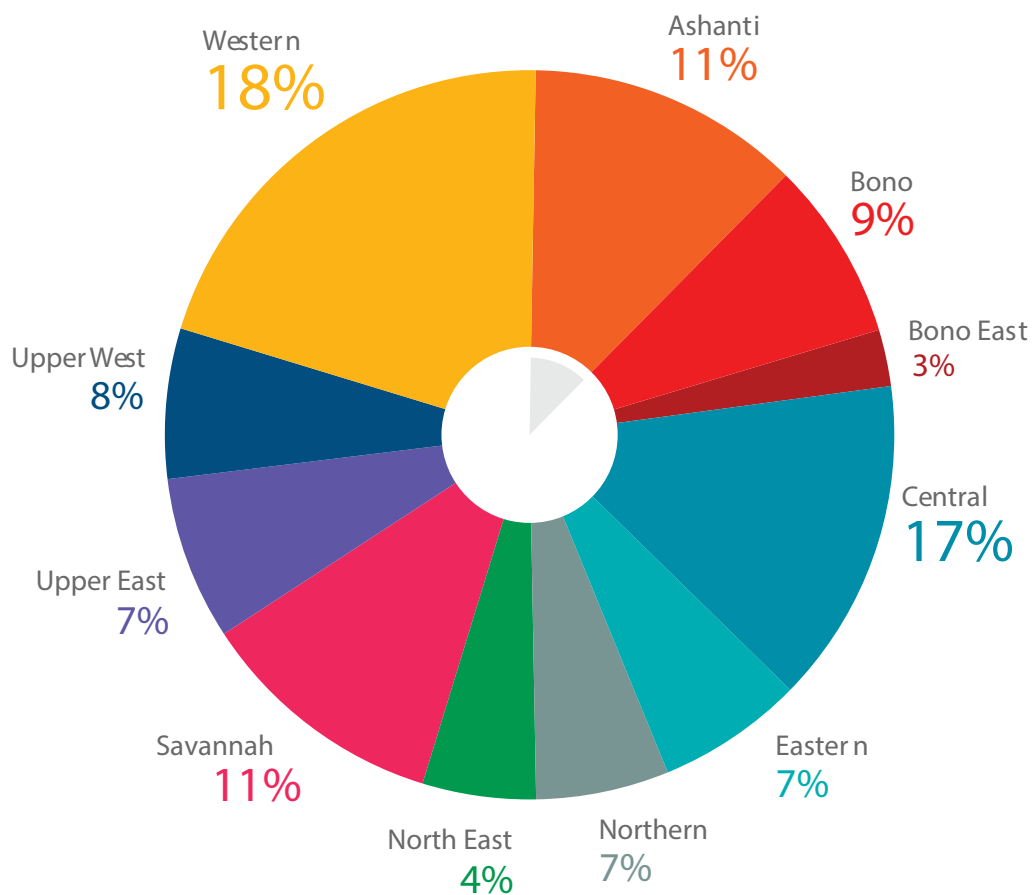
Despite the challenges presented by the COVID-19 pandemic, the National Cyber Security Centre team ensured successful planning and execution of the regional activities.

Data Representation of Regional Sensitisation Exercise Participation

S/N	REGION	TARGET GROUP	NUMBER OF PARTICIPANTS	REGIONAL TOTAL
1	Ashanti	RCC GJA	85 45	130
2	Bono	RCC GJA	45 60	105
3	Bono East	RCC	40	40
4	Central	RCC Rotary Club Youth Engagement	75 20 110	205
5	Eastern	RCC GJA	50 35	85
6	Northern	RCC GJA	45 42	87
7	North East	RCC	50	50
8	Savannah	RCC Youth Engagement	105 25	130
9	Upper East	RCC GJA	60 25	85
10	Upper West	GNAT	94	94
11	Western	RCC GNAT Youth Engagement	87 44 93	224
Total				1235

RCC – Regional Coordinating Council
GJA – Ghana Journalists Association
GNAT – Ghana National Association of Teacher

% of Regional Participation out of Nationwide Total



Conclusion

The 2020 edition of the National Cyber Security Awareness Month (NCSAM) under the theme, Cybersecurity in the Era of COVID-19 sought to highlight the key interventions and investments made to demonstrate the country's cybersecurity readiness in the pandemic era. The month-long event which leveraged on the successes of the previous editions consisted of high-level programmes and regional events strategically targeted at key public and private sector institutions, businesses, civil society groups, the media, and the general public. Activities were conducted via workshops, forums, presentations, media interviews and seminars. Participation was in a hybrid format comprising physical engagements and the utilisation of virtual platforms.

The formal opening of NCSAM 2020 was on October 1, 2020 and it was an opportunity to launch the Internet Watch Foundation Child Online Protection (COP) Reporting Portal. The portal is a major intervention that seeks to address challenges faced in the takedown of Child Sexual Abuse Materials for online channels. It seeks to complement the already existing Cybercrime/Cybersecurity Incident Reporting Points of Contact in the collation and resolution of all cyber-related incidents and suspected vulnerabilities within the cybersecurity ecosystem.

Regional cybercrime/cybersecurity sensitisation exercises were organised across the sixteen regions of Ghana. The entire sensitisation exercise reached out to over 1,500 participants from the Regional Coordinating Councils (RCC), Ghana Journalists Association (GJA), Ghana National Association of Teachers (GNAT), civil society and professional groups, the media, and the public. These awareness creation and capacity building activities further consolidated and re-affirmed the NCSC's commitment to cybersecurity development.

The High-level events were conducted to extensively cover the four thematic areas of the Safer Digital Ghana Campaign i.e., Children, the Public, Businesses, Government. The activities were scheduled weekly with each week dedicated to a thematic area. The events comprising roundtable forums, workshops, and seminars witnessed the participation of about 200 participants from governmental and non-governmental institutions, industry players, the media fraternity, civil society groups, academia, international partners, and Ghana's diplomatic corps. The key activity that climaxed the high-level event was the Launch of the Security Operations Centre (SOC) at the National Information Technology Agency (NITA) to augment the country's cybersecurity operations and incident response capabilities.

The month-long event which sought to assess Ghana's cybersecurity readiness at the national, regional and global levels in the era of the COVID-19 proved to be unique with an increase in scope and reach with regards to capacity building and awareness creation compared to the previous editions.

The Ministry of Communications extends its gratitude to all stakeholders, sponsors and partners for their immense support and financial commitment that led to the successful organisation of the event and most importantly towards the development of the country's cybersecurity for A Safer Digital Ghana.

Recommendation

Below are some of the key recommendations made during the NCSAM 2020:

- ➔ Cybercrime and cybersecurity education must be incorporated into the curriculum of all levels of education in the country as a subsidiary of ICT.
- ➔ Capacity building efforts must be intensified for relevant state and private institutions.
- ➔ The awareness creation exercise must be further increased in scope and conducted throughout the year.
- ➔ Cybersecurity education should be targeted at every district nationwide and must be conducted regularly.
- ➔ Cybersecurity clubs should be established in schools to increase awareness creation efforts.
- ➔ There should be increased capacity building for ICT educators.
- ➔ Citizens must develop a positive cybersecurity culture of reporting suspected incident or incidents and utilise the available PoC platforms.
- ➔ Training on Cybercrime and e-Evidence handling should be integrated into the curricular of the judicial training institute.
- ➔ Police officers must have basic knowledge in cybercrime and electronic evidence handling to enhance their investigations in cyber-facilitated crimes.
- ➔ Organisations are to have a framework for risk mitigation.

Photo Gallery



Photo Gallery



Photo Gallery



Photo Gallery



Photo Gallery



Planning Phase

As part of preparations towards the 2020 edition of the National Cyber Security Awareness Month (NCSAM), a Planning Committee was constituted to oversee to the coordination, implementation of ideas, vision and goal of the National Cyber Security Awareness Month.

Five (5) Sub-committees were formed out of the planning committee comprising:

- ➔ Programmes and Content sub-committee
- ➔ Budget and Sponsorship sub-committee
- ➔ Communications, Media and PR sub-committee
- ➔ Event, Logistics and Organizing sub-committee
- ➔ Reporting & Editorial sub-committee

About Us

The National Cyber Security Centre (NCSC) is a national agency established in 2018 under the Ministry of Communications. The NCSC is responsible for Ghana's cybersecurity development including cybersecurity incidents response coordination within government and with the private sector. The NCSC is responsible for Awareness Creation & Capacity Building, Cybersecurity Incident Coordination & Response (CERT), Critical Information Infrastructure Protection (CIIP), Child Online Protection, and International Cooperation, among others. The NCSC is responsible for the development and implementation of Ghana's National Cybersecurity Policy & Strategy. The NCSC work closely with the National Cyber Security Technical Working Group (NCSTWG) in the implementation of cybersecurity initiatives across government and non-governmental sectors.

Partners & Sponsors

PARTNERS



ORGANISING PARTNERS



MEDIA PARTNERS



SPONSORS





NATIONAL
CYBER SECURITY
CENTRE

Securing Ghana's Digital Journey...

Whatsapp: 050 160 3111

Mobile App:
NCSC Ghana



**CYBERCRIME/
CYBERSECURITY
INCIDENT
REPORTING
POINTS OF
CONTACT**



E-mail:
report@cybersecurity.gov.gh

Call: 292



SMS: 292



Online Form:
www.cybersecurity.gov.gh/report

National Cyber Security Centre

3rd Floor, NCA Tower
KIA, 6 Airport By-pass Rd., Accra
Digital Address: GL-126-7029

Tel: +233 050 3185846
E-mail: info@cybersecurity.gov.gh
www.cybersecurity.gov.gh