GHANA CHAMBER OF TELECOMMUNICATIONS
M-Powering People. SIMpacting Lives

OPENING REMARKS BY DR. ING. KENNETH ASHIGBEY, CEO OF GHANA CHAMBER OF TELECOMMUNICATIONS AT THE 17TH KNOWLEDGE FORUM AT THE LABADI BEACH HOTEL, LA ON WEDNESSDAY JULY 7, 2021 – TOPIC - THE NEW CYBERSECURITY LAW: ITS IMPLICATION ON PEOPLE AND BUSINESSES

The National Cyber Security Advisor – Dr. Albert Antwi-Boasiako
Members of the Ghana Chamber of Telecommunications
Invited Guests
My Colleagues from the Media
Distinguished Ladies & Gentlemen

I would like to welcome you all to the 17th Edition of our quarterly knowledge fora geared towards influencing, educating and stimulating deep discussions related to the mobile and ICT industry with the main objective of improving understanding of industry topical issues.

Our topic today which is on Ghana's new Cyber Security Law, The Cyber Security Act, 2020 (Act 1038), for us is a critical piece of legislation that holds a lot of promise for us in the current 4th industrial revolutionary era of digital transformation. So, it is very important we do not make this discussion a technical conversation but we will seek to demystify all legal and technical jargons in the context of our subject matter. In summary, we are seeking to provide answers to lingering questions around the new law, as well as enable the public appreciate further the importance of Act 1038 in their lives and that of the country.

Permit me to congratulate the Hon. Minister for Communications and Digitalization and her team at the National Cyber Security Centre led by our keynote speaker Dr. Albert Antwi-Boasiako for the significant feat of being ranked 3rd in Africa by the ITU.

Ghana scored 86.69 per cent for secure cyberspace and comes behind Mauritius and Tanzania in that order. For me the significance of achievement is not just in the fact that Ghana leaped frogged from 11th position to 3rd place but also the fact that we attained high score of 87% from as low as 33% and 44% in as recently as 2017 and 2018 respectively

This would tell the world that we are ready for 4th industrial revolution business. This is not only good for government but also for private sector and especially our industry. I am sure that the passage of the Cybersecurity Act, 2020 (Act 1038) to provide a legal basis for the country's cybersecurity development and the institutionalisation of cybersecurity to foster domestic cooperation and collaboration would have contributed to Ghana attaining 87% overall aggregated score when measured according to the five strategic pillars of the ITU's Global Cybersecurity Agenda (GCA) - legal measures, technical measures, organisational measures, capacity building and international cooperation.

Dr. Albert Antwi-Boasiako, please convey to the honorable minister our congratulations and the commitment of the

members of the Ghana Chamber of Telecommunications to continue to work with you to ensure that we maintain our acceleration and attain the 100% status in the near future. The 1st position globally is in reach, it would require the continued collective and collaborate leadership that has brought us this far.

Over the course of just a few decades, the world has entered a digital age. People from all over the planet are connected online. By way of comparison: in 1996, only 36 million people used the internet, about one per cent of the world's population. By the end of 2020, more than 4.5 billion people now use the internet, while social media users have passed the 3.8 billion mark.
Putting this in further perspective, nearly 60 percent of the world's population is already online, and the latest trends suggest that more than half of the world's total population will use social media by the middle of this year.

But the boundless opportunities of digitalisation come with serious challenges: digital development without cybersecurity is not sustainable. You cannot rely on a tool that is not secure and cannot be trusted. And digital development cannot flourish when lack of support for the norms of responsible behaviour is undermining global stability.

The recent sprawling ransomware attack that hit hours before the beginning of the July Fourth holiday weekend by REvil, the

same Russian-language group who are demanding $70 million to unlock the thousands of businesses affected by the hack. This same group are behind the attack on meat processor JBS. This is a major challenge that the world has to grapple with. With the Fourth Industrial Revolution shifting into high gear, such threats of malicious cyber activities is keeping pace with the opportunities presented by AI, 5G, 6G and quantum computing.

Ghana passed the landmark Cybersecurity Act at the end of the year 2020. The National Cyber Security Centre (NCSC) is expected to transition into the Cyber Security Authority (CSA) in the coming weeks, per Section 2 of the Act 1038, to regulate cybersecurity activities in the country and further lead Ghana's cybersecurity development.

The Law as we know it would also lead to the protection of critical information infrastructure of the country, regulate cybersecurity activities and offer the protection of children on the internet as well as developing Ghana's cybersecurity ecosystem. We are also aware that this new law is also targeted at positioning Ghana to prevent, manage and respond to cybersecurity incidents in view of our digital transformation agenda.

As an industry we were graciously tied to the processes that led to the development and passage of this law. Indeed, the tireless and strenuous efforts showcased by the team at the National Cyber Security Centre cannot go without mention by the industry

and we are continuously grateful for their show of professionalism and commitment to work with the industry in actioning the core components of the Act.

An important declaration by the new law in classifying telecommunications and ICT infrastructure as Critical National Information Infrastructure is key for the growth and sustainability of the mobile industry. It is important to state that the mobile industry is today reeling under the menace of fibre cuts, diesel thefts, vandalism and thefts of equipment's delivering service to millions of Ghanaians by the second.

We would want to sound a note of warning to all Road Contractors and other stakeholders who operate within the Right of Way including the Contractors on the Beach Road Project just a few kilometers from here that their days are numbered and if they do not stop the reckless destruction of our fibre cables they would find themselves at the wrong side of Act 1038

A declaration by the Authority when setup, leveraging the existing law will ensure that, there should be no tampering with the public core of the internet. Internet infrastructure should be regarded by everyone as the backbone of modern society. Undersea cables and other vital elements should be off limits and safeguarded by all. For an industry that provides vital communication, and support in numerous sectors including driving financial inclusion, we trust this might not be too much to ask for!

We are looking forward to other key discussions in areas of Administration of the Authority as well as working with the Authority and other existing Regulators to tackle and manage any potential bureaucracies that may stifle growth within multiple sectors of the economy when the Centre expands its reach and activates fully its objectives and goals.

Cyber threats don't respect national borders. They are as transnational as, say, climate change or the ongoing global pandemic COVID-19. Therefore, it's not enough to address threats solely at national level, or in a single regional organisation. That is why Ghana's enactment of the new law is commendable and crucial to position it within the global bloc of nations keenly working towards the fight against Cyber Crime.

A stable cyber domain contributes to a more stable society, a more stable democracy, and a more stable business environment.

In conclusion, ladies and gentlemen, and our friends from the media. The name of the game is international, multi-stakeholder collaborations and partnerships. Within Ghana, as we are doing today, we will work together to boost resilience, set the rules of the road, improve the attribution of malicious acts, and hold those responsible to account and secure our digital space.

To serve the cause of freedom and justice, these words at Independence meant that all Ghanaians, men, women, old and young – have the right to enjoy life, liberty and the opportunity

to pursue happiness as they chose and within the laws of our country.

A safe digital Ghana, clearly is in line with our National motto.

To end, as we, our colleagues and families remain safe and healthy, conscious of the fact that COVID-19 is still with us. We should use our current circumstances to strengthen our organizations, making them more resilient and conscientious, and elevate your professional offering by using the time and available resources to upskill and advance.

Thank you all.
God Bless Our Homeland Ghana

Crypto Ransom Payments Skyrocketed in 2020

Felix Richter
Data Journalist
felix.richter@statista.com

Up to 1,500 businesses around the world have been affected by a large-scale ransomware attack targeting a popular IT management tool from U.S. software vendor Kaseya. The targeted software, a tool called VSA, is widely used by IT service providers to manage the IT infrastructure of smaller firms, making it harder to gauge the total impact of Friday's attack.
"To date, we are aware of fewer than 60 Kaseya customers, all of whom were using the VSA on-premises product, who were directly compromised by this attack. While many of these customers provide IT services to multiple other companies, we understand the total impact thus far has been to fewer than 1,500 downstream businesses," Kaseya wrote in a statement on Monday, advising customers to keep VSA Servers offline until further notice.
According to a Reuters report, the attack paralyzed mostly small businesses around the world, with a Swedish supermarket chain forced to close hundreds of stores among the larger victims. The group claiming responsibility for the attack, a Russian-linked cyber crime collective called REvil,

have demanded $70 million to restore the data they're holding ransom, making it one of the largest ransomware attacks to date.

Ransomware attacks have become more common and increasingly costly over the past few years. According to Chainalysis, a blockchain data platform tracking cryptocurrency payments to known ransomware addresses, victims paid more than $400 million in ransom last year, marking a 337-percent jump from the 2019 total. "2020 will forever be known as the year of Covid, but when it comes to crypto crime, it's also the year that ransomware took off," Chainalysis writes in its 2021 Crypto Crime Report. As the following chart shows, ransomware attacks show no signs of easing in 2021. In the first five months of the year, victims already transferred more than $80 million to cyber criminals, almost matching the total for the entire year of 2019.