2022 CYBERSECURITY CONFERENCE

Strengthening Nigeria's Cybersecurity Ecosystem and Protecting Today's Hybrid Workplace

OCTOBER 6, 2022
12:00PM WAT | 7: 00 AM EST

ORGANIZERS: AMERICAN BUSINESS COUNCIL Promoting Nigeria-America Economic Partnership; COMERCiO

PARTNER: Naijasecforce

SPONSORS: hp; DELLTechnologies

OUTCOMES REPORT

AMERICAN
BUSINESS COUNCIL
Promoting Nigeria-America Economic
Partnership

The mission of the American Business Council is to support sustainable socio-economic reform initiatives in Nigeria through public policy advocacy, promotion, and implementation. This Outcomes Report is part of a partnership between the American Business Council, Partners, and Sponsors of the 2022 Cybersecurity Conference.

Sponsors and Partners

American Business Council thanks sponsors and partners for making the Conference memorable.

Table of Contents

Remarks by ABC President

We welcome the Honourable Minister Professor Isa Ali Ibrahim Pantami, the US Ambassador to Nigeria Mary Beth Leonard and the Minister of ICT and Innovation for Rwanda, Paula Ingabire and other very important stakeholders here. American Business Council, the Federal Ministry of Communications and Digital Economy, Office of the National Security Adviser as well as Commercio decided to focus this year on "Strengthening the Cybersecurity Ecosystem and Protecting the Hybrid Workplace."

In 2021, the American Business Council held the 1st Cybersecurity Conference and recommended, among others, for international collaborations, capacity building, clear standards for data flow privacy and protection standards, online child protection and reporting channels to improve the cybersecurity landscape in Nigeria.

The cybersecurity space remains critical to governments and the private sector not just in Nigeria but in Africa especially with the increase in cybercrime resulting from the new normal work style occasioned by the COVID 19 pandemic.

Cloud computing platforms have altered how organizations utilize, share and store information. While these platforms enabled a transition to a hybrid workplace, they also face great threats and would require sufficient security to prevent data theft.

Overall, the Council remains committed to working with government and other stakeholders to drive positive conversations like this one that will engender confidence about the business environment and encourage investors. In addition to providing an avenue for the federal government to share updates on its cybersecurity regulatory framework and collaboration with private sector, it also opens up avenues for the private sector to recognize the new opportunities in the cybersecurity space.

Dipo Faulkner
President,
American Business Council

Background

Theme: *Strengthening Nigeria's Cybersecurity Ecosystem and Protecting Today's Hybrid Workplace*

The cybersecurity space has become of critical importance to governments all over the globe, and the government of Nigeria is no different. Cybersecurity, the Soft Infrastructure Pillar in Nigeria's National Digital Economy Policy and Strategy, is a crucial pillar which outlines a vision for diversifying the country's economy, using digital technologies as a catalyst.

The COVID-19 pandemic has accelerated the adoption of digital platforms, leading to a significant increase in cyber threats, and this has proved costly to economies across the globe, including the African economy. For instance, Cybersecurityventures estimates that global cybercrime will cost $10.5 trillion by 2025[1] and according to Resecurity, Africa loses $3.5 billion annually to cybercrime[2].

In the past, people under 20 were the most resilient to cybercrimes but with the pandemic and the migration of more children to online schooling platforms, there was a 100 percent increase in this age demographic falling victim to cybercrime. Cybercrime victims in their teens increased from 10,000 per year to 20,000 from 2019 to 2020. This underscores the urgent need for tighter online child protection measures and a commitment to make deliberate efforts to create more awareness and increase advocacy in the nation's cybersecurity ecosystem.

Cybercrime earns cyber criminals $1.3 trillion every year[3] and the average cost of a data breach on remote work is about $137,000 per attack[4]. With more organizations adopting the hybrid workplace, the need for cyber security is made even more evident.

Also, cloud computing platforms have altered how organizations utilize, share and store information. Though these platforms have provided huge benefits, they however face great threats. Attacks on such platforms have rapidly increased, accounting for 20 percent of all cyber-attacks in 2020. Consequently, threats to cloud infrastructure cannot be ignored and the need to provide sufficient security to prevent data breeches is of utmost

[1] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] https://www.businesslive.co.za/fm/fm-fox/2022-02-18-native-35bn-and-growing-the-huge-cost-of-cybercrime-in-africa/

[3] https://learn.bromium.com/rprt-web-of-profit.html

[4] https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

importance.

Nigeria's cyber ecosystem comprises different participants- the government, the private sector, individuals, cyber devices and processes, all which interact with diverse purposes. The sustenance of such an ecosystem is heavily dependent on the regulations, frameworks and policies that undergird the system. Therefore, it is necessary that the government creates the right policies to enable the system to thrive.

The 2021 Nigerian National Cybersecurity Policy and Strategy (NCPS) identifies the banking, finance, and insurance sector as some of its thirteen critical information infrastructure sectors. The NCPS presents the Nigerian government's approach to protecting these kinds of critical information infrastructure.

The Central Bank of Nigeria (CBN) established the Consumer Protection Department in April 2012 to develop and implement an effective consumer protection framework and promote consumer confidence in the financial system. The Department performs three primary functions, namely complaints management, market conduct and development, and consumer education and financial literacy.

In 2021, American Business Council Nigeria, the Ministry of Communication and Digital Economy, USTDA and Commerio held the 1st Cybersecurity Conference and recommended among others for international collaborators, capacity building, clear standards for data flow privacy and protection standards, online child protection and reporting channels to improve the cybersecurity landscape in Nigeria.

A cybersecurity landscape that grows ever more threatening needs a strong pro-active and well-equipped ecosystem that will provide participants with the most benefits and the least threats. Hence, all stakeholders would need to step up to their responsibilities while also adopting a collaborative approach to strengthen the ecosystem.

The Cybersecurity Conference has the following objectives:

1. Provide an avenue for the Federal Government to share updates on its cybersecurity regulatory framework with the private sector while also addressing the lack of policy and regulation for cryptocurrency.
2. Provide an avenue for the private sector to recognize the new opportunities in the cybersecurity space.
3. Promote the idea of a Cyberhub project among stakeholders, with the aim of building capacity across the six geopolitical zones via introduction of curriculum inter alia and providing cybersecurity jobs that will not only be globally competitive but will also help address

the brain drain challenge experienced in the cyber space.

4. Encourage public-private partnership in capacity building and encourage the creation of mentorship programs.
5. Provide private sector input for driving framework developments and laws for other emerging technologies that support cybersecurity, such as Artificial Intelligence and Blockchain.
6. Identify the current landscape on regulations for the protection of children online and receive input from technology companies on their activities in that area.
7. Highlight the need for more awareness and advocacy in the cybersecurity ecosystem..

Keynote Remarks by the Honourable Minister of Communications and Digital Economy

Introduction

I am delighted to deliver this Keynote Address at the 2022 Cybersecurity Conference organised by the American Business Council. It is commendable that you are organising the 2nd edition of this event, following the one you organised on the 24th of August, 2021. The pedigree of the speakers, panelists, partners and sponsors shows the high level of importance that we all attach to the issue of cybersecurity, and rightly so.

The theme of this Conference is "Strengthening Nigeria's Cybersecurity Ecosystem and Protecting Today's Hybrid Workplace." This is a very pertinent theme and it gives us the opportunity to discuss the new post-COVID realities of the future of work. Prior to the COVID-19 pandemic, the rate of cybercrime was already staggering. As expected, the pandemic was a catalyst, not just for the adoption of digital platforms, but also for the increase in the opportunities for cybercrime.

Importance and Impact of Cybersecurity

The pace of innovation, the growing level of interconnectivity in the digital environment, as well as our "new normal" of high dependence on technologies has created a society that is exposed to security threats which are more numerous, highly networked, more widely distributed, very adaptive, and can be quite difficult to isolate and deal with.

The COVID-19 pandemic brought about this new normal, that is the hybrid workplace, and this is something that has now become the default mode for work in the Fourth Industrial Revolution. The growth in the number of virtual conferences, such as this one, and the growth in the adoption of virtual meeting platforms has been very significant and there is no sign that this trend would change in the near future.

According to the International Telecommunication Union (ITU), within two years of the pandemic, close to 800 million new users (about 10% of the global population) connected to the Internet during the COVID-19 pandemic. In Nigeria, there were about 16 million new connections to the Internet. The greater access to the Internet and to digital platforms enabled remote collaboration, remote education, e-commerce services, telemedicine and other useful applications. Africa is also set to benefit from a growing digital culture, as the United Nations estimates that 230 million new digital jobs can be created in sub-Saharan Africa, leading to an increased revenue of $120 billion by 2030.

However, it is noteworthy that the gains of going digital are countered by the pains of being exposed to cyberthreats. For example, studies estimate that cybercrime already costs African economies over $3 billion annually and the United Nations estimates that cyber breaches would cost $5 trillion by 2024- a staggering 28% of the Gross Domestic Product (GDP) of the European Union.

Furthermore, according to the Chief Technologist – Security and Privacy for Personal Systems for HP— Dana Lengkeek, in 2018 noted that "a new piece of malware is released every day within 4.2 seconds." This pre-pandemic assessment translates to 144,000 malwares in just one week and the current statistics are expected to be much higher than this. The foregoing paints a grim picture and makes a strong case for the promotion of cybersecurity strategies to counter such cyberthreats.

The first half of the theme talks about the need to strengthen the cybersecurity ecosystem and this is very important. First of all, we are reminded that a great amount of our efforts should be focused on strengthening cybersecurity, rather than merely addressing cybercrime. When we develop the capacity of our citizens and increase cybersecurity awareness in the country, then we can reduce the incidence of cybercrime. This is why I am happy that a cybersecurity hackathon preceded this Conference and I am pleased that the Conference is taking place in October- a month that is dedicated to Cybersecurity Awareness.

Cybersecurity lays an emphasis on a proactive approach to addressing these cyberthreats and it is common practice to utilise models to assess how prepared an institution is to ward off cyberattacks. A cybersecurity maturity model enables countries to carry out a top-level assessment of their level of preparedness and to identify the gaps that need to be addressed.

Furthermore, the mention of the word ecosystem goes to show that any sustainable cybersecurity effort needs to integrate different stakeholders in an ecosystem. Our cybersecurity ecosystem is made up of both the public and private sector, as well as the citizens, the regulators, Office of the National Security Adviser, academia, students, etc.

I led Nigeria's delegation to the International Telecommunication Union Plenipotentiary Conference in Bucharest, Romania and we had a very successful outing. During my presentation of Nigeria's Policy Statement at the plenary, I made a number of recommendations which were well received by the member states and participants. The recommendations are relevant to the theme of this Conference so I will mention them here:

As we head into the post COVID-era, we have a few recommendations:

i. Prioritising cybersecurity and cyberimmunity by encouraging members to actively share global statistics;
ii. Promoting policies, research and partnerships that foster the inclusive and ethical use of emerging technologies;
iii. The metaverse extends our physical world to the virtual and it is important for member states to collaborate to ensure that the regulatory environment for the physical world is also adapted for the virtual world; and
iv. We call on member states to be active participants in the discussions on the WSIS Action Lines and in the implementation of its outcomes.

Initiatives for Strengthening the Cybersecurity Ecosystem and Protecting the Hybrid Workplace

I have a very high level of interest in cybersecurity for Nigeria and other African countries and this motivated me to write a book to document our efforts in strengthening Nigeria's cybersecurity ecosystem. This book is entitled "Cybersecurity Initiatives for Securing a Country" and it was unveiled to the public on the 14th of July, 2022. One of the chapters of the book gives a model for strengthening the cybersecurity of any country. I will discuss some of them superficially.

The initiatives listed are as follows:

1. Develop a National Digital Economy Policy to serve as the overarching policy for issues relating to cybersecurity;
2. Conduct a baseline study to identify the main cyberthreats and the key elements of the cybersecurity ecosystem;
3. Develop a National Cybersecurity Policy/Law;
4. Establish a National Cybersecurity Centre, to include a Shield to Scan and provide a Safety Score for Government and Critical Private Websites;
5. Enhance Data Protection and Privacy and support for the accelerated implementation of a Digital Identity Programme;
6. Make digital identity mandatory for all citizens and legal residents;
7. Establish and utilize Internet Exchange Points;

8. Establish cybersecurity departments/units in key public and private institutions;
9. Establish national and sectoral Computer Emergency Readiness and Response Teams (CERRTs);
10. Enhance and protect Critical ICT National Infrastructure;
11. Build capacity in cybersecurity and support advocacy and innovation;
12. Introduce Elementary Cybersecurity Courses for students from the primary to the tertiary education levels; and
13. Prioritise collaboration.

Conclusion

I would like to conclude by reiterating our commitment to strengthening Nigeria's cybersecurity ecosystem and we encourage stakeholder engagements and collaborations like these. Thank you for your kind attention and I wish you very successful deliberations.

I. Building a Resilient Cybersecurity Ecosystem in Nigeria

The first panel of the event focused on the benefits and challenges associated with the growing adoption of hybrid workplace models. These models allow people to work at physical offices and also remotely. Though this provides flexibility for workers and their employers, it also increases the attack surface for cyberattacks. The panel addressed this new risk, vulnerabilities and its impact on the cyber ecosystem in Nigeria and Africa.

Panelists

- Prof. Isa Ali Ibrahim (Pantami), FCIIS, FBCS, FNCS, Honorable Minister, Communications and Digital Economy;
- HE Paula Ingabire, Honorable Minister of ICT and Innovation, Rwanda;
- Major General Samad Akesode, Director of Communications, Office of the National Security Adviser;
- Matthew Klein, Director, Coursera's International Public Sector Practice.
- Mr. Terlumun George-Maria Tyendezwa, CFE, Federal Ministry of Justice
- <u>Moderator:</u> Honourable Dr. Emeka Ujam

The Honourable Minister of Communications and Digital Economy of Nigeria was asked about the role of the *triple helix model which emphasizes the importance of collaboration between government, academia and the industry*. The focus was to get Prof. Pantami's perspective on the relevance of this model in Nigeria and what parallels can be drawn between the triple helix model and Nigeria's cybersecurity context.

Prof. Pantami noted that Nigeria is currently implementing the triple helix model. He noted that the necessity of the implementation of the triple helix model can be seen in the Federal Government's approach to the implementation of policies and regulations in the digital economy sector. In particular, through this enabling environment, the Federal Government of Nigeria is supporting the academia as they carry out research and development. As part of the adoption of the triple helix model in Nigeria, the industry is also supported to ensure the success of the sector and implementation of the research conducted. He noted that the digital economy sector is enhanced by the adoption of the triple helix model, for which the roles of the government, academia and the industry are intertwined. He emphasized the importance of always bringing together government, academia and industry for a more effective result.

The Honourable Minister of ICT and Innovation of Rwanda was asked about *her role as a woman in leading digital transformation efforts in Rwanda, in light of women's capacity to make a big difference in information and communication technology*. She was also asked about her approach to getting more women into the tech ecosystem.

Her Excellency Paula Ingabire emphasized how a focus on the development of skills has assisted women in Rwanda. She noted that in Rwanda, women are "presented with the opportunity of reskilling and upskilling without having to go through a degree program to gain a particular skill set." She further noted that in Rwanda, at an early age, girls who are good in mathematics and physics are given an opportunity to join a Science, Technology, Engineering and Mathematics (STEM) or cybersecurity career and are groomed to excel. The Minister stated that it is challenging in the workplace for women to combine the roles of being a wife, mother and certain work schedules, so there is the need for workplace retention policies to make it easier for women and girls.

Furthermore, she noted the importance and urgency of getting more women to play a greater role in policy formulation and implementation with regard to cybersecurity. She also stressed the importance of inclusivity and diversity in the digital economy agenda of countries in the African region. She urged policy makers to think outside the box while formulating programmes to empower women and make them part of the cybersecurity decision making process. Her Excellency, Paula Ingabire, also mentioned this in light of the fact that women are said to make up just 24% of the global cybersecurity workforce, even though they make up 51% of the global workforce.

Online learning platforms have become a medium of choice for enhancing digital skills. As such Matthew Klein, Director of Coursera's International Public Sector Practice, was asked to *share some key approaches for accelerating the massive adoption of online platforms in developing countries.*

Mr. Klein noted that Coursera's success is due to their focus in developing high quality content from any part of the world for its 100 million clients across 100 countries. For example, in cybersecurity, Coursera uses best-in-class content from IBM and content from other top institutions as Google, Facebook, etc. Other strategies used include a focus on the needs of the job, training and feedback, and lastly, collaboration.

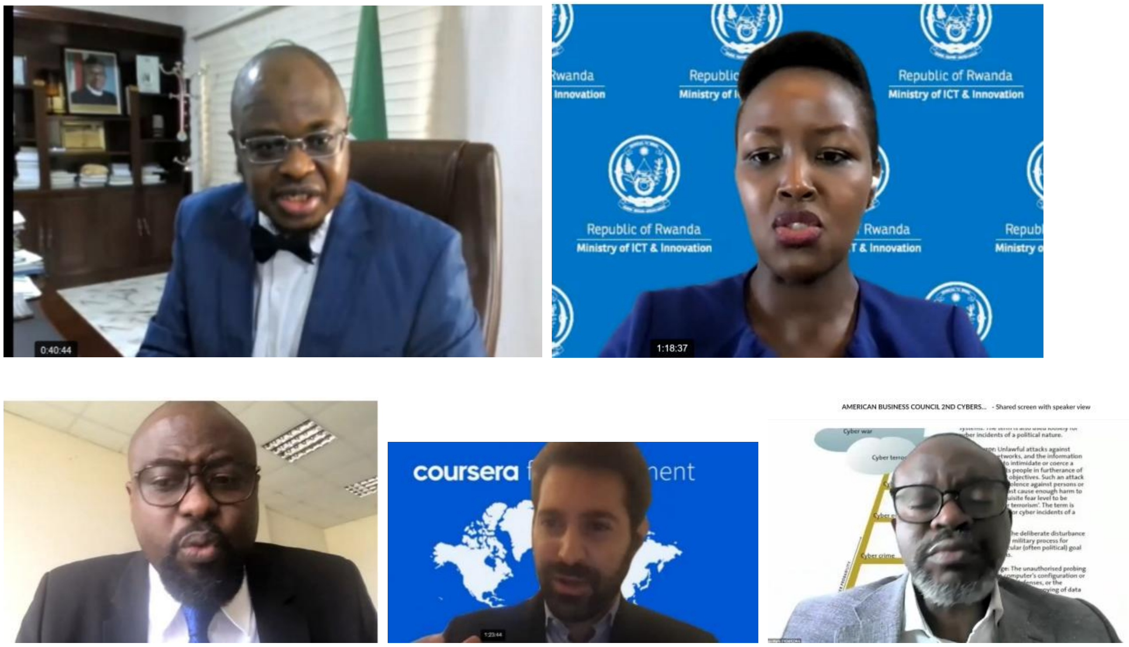
He noted interesting examples, such as in Costa Rica, where the private sector is carried along in the training process. In this example the participating institution and the students give regular feedback to the organizers of the training with a view to significantly enhancing the programme. He also talked about the learner journey and how it is important to encourage the students to take advantage of the opportunities that these training programmes provide. Mr Klein also added that there is a need for inter-ministry collaboration like the one practised by Ghana and Kyrgyzstan.

The Director of Communications, Office of the National Security Adviser (ONSA), was asked about *the proposed amendment of the Cybersecurity Act and the framework to implement the National Cybersecurity policy and strategy*. In his reply, Major General Samad Akesode stated that ONSA provides strategic guidance for cyber security activities in the country and recently, the cyber security policy and strategy was reviewed by President Muhammadu Buhari. The amendment of the Cybercrime Act is one of the key initiatives for implementation of these strategies.

The representative of the Federal Ministry of Justice was asked how the Ministry is *working with other security advisers to combat cybercrime*. In his reply, Mr. Terlumun George-Maria Tyendezwa stated that the Federal Ministry of Justice and the Office of the National Security Adviser have been working together particularly in the area of capacity building. Another area of collaboration is the use of the law to identify and track cybercriminals. He noted that the Ministry has also followed through on the admission of Nigeria into the International Committee of Nations Fighting Cybercrimes.

Her Excellency Paula Ingabire was also asked about *the importance of women in* *policy making when it comes to national issues relating to the development of the digital economy.*

According to Honourable Paula Ingabire, it is not only important but also a matter of urgency to identify some of the practical examples or things that can lead to a more inclusive and diverse leadership in the digital economy sector, not just in policy making but also at the implementation level. For Rwanda, in terms of policy making, there is a population of 51% of women in the cabinet and more than 62% in parliament. It is not just at the policy level but there is also some diversity in the private sector and corporate world or tech industry and how we see more women take up roles in creating solutions, in addition to their roles as decision makers.


0:40:44
Republic of Rwanda
Ministry of ICT & Innovation
1:18:37
coursera
AMERICAN BUSINESS COUNCIL 2ND CYBERS... - Shared screen with speaker view

L-R: (Top): Prof. Isa Ali Ibrahim (Pantami), HE Paula Ingabire; (Bottom): Dr. Ujam, Mr. Matthew Klein, Mr. Terlumun George-Maria Tyendezwa

Awards Session

As part of the 2nd Cybersecurity Conference, the Honourable Minister of Communications and Digital Economy announced the awards for the winners of a cybersecurity-focused Hackathon. The American Business Council Nigeria and Comercio Limited (a leading information technology solution provider in Nigeria) in partnership with NaijaSecForce, organized a "Capture The Flag" contest as part of the 2022 Cybersecurity Conference and it took place in the weeks leading to the Conference.

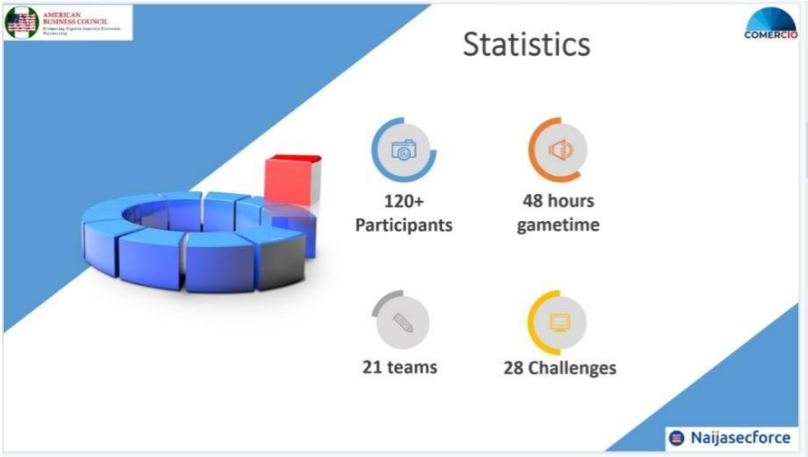
The objective of the hackathon was to highlight the capacity in the Nigerian Cybersecurity space and show the importance of implementing a cybersecurity framework in Nigeria.

Over 120 individuals participated in the hackathon across 21 teams. There were 28 challenges that took place over a 48-hour game-time. At the end of the competition, the following 3 teams were selected as winners:

1. REDHAT-NG
2. AKATSUKI
3. THE BLACK BULLS

The members of the REDHAT-NG were given laptops from HP and Dell. One of the partners, Zenith Bank, offered all the members of the first 2 winning teams cybersecurity trainings valued at up to $500 dollars. Promotional materials from HP and American Business Council were also offered to the members of the second and third winning teams.

In his brief remarks, the Honourable Minister commended the ABC for the initiative. He urged the participants that did not win any prizes not to see themselves as losers but to view the hackathon as an opportunity to develop themselves in the area of cybersecurity.



Statistics

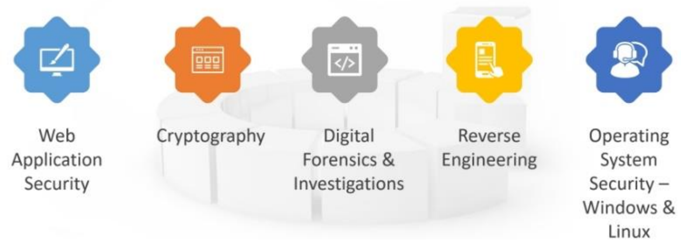
120+ Participants

48 hours gametime

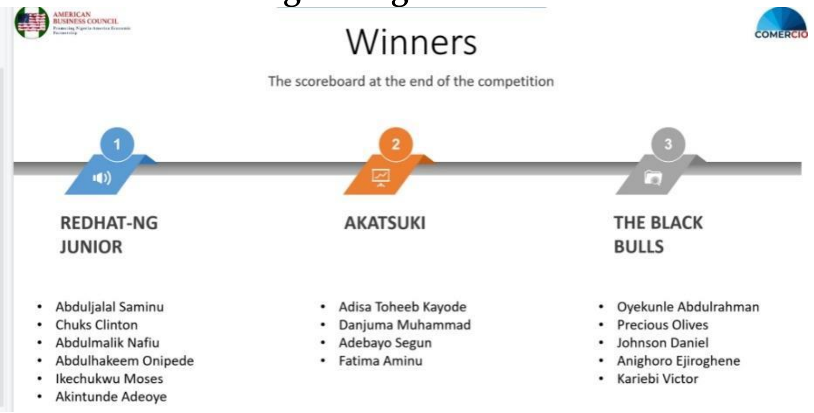
21 teams

28 Challenges

Statistics from the Hackathon


Web Application Security
Cryptography
Digital Forensics & Investigations
Reverse Engineering
Operating System Security – Windows & Linux

Hackathon Challenge Categories



Winners

The scoreboard at the end of the competition

1 REDHAT-NG JUNIOR

- Abduljalal Saminu
- Chuks Clinton
- Abdulmalik Nafiu
- Abdulhakeem Onipede
- Ikechukwu Moses
- Akintunde Adeoye

2 AKATSUKI

- Adisa Toheeb Kayode
- Danjuma Muhammad
- Adebayo Segun
- Fatima Aminu

3 THE BLACK BULLS

- Oyekunle Abdulrahman
- Precious Olives
- Johnson Daniel
- Anighoro Ejiroghene
- Kariebi Victor

Teams and Members of the Three Winners of the Hackaton

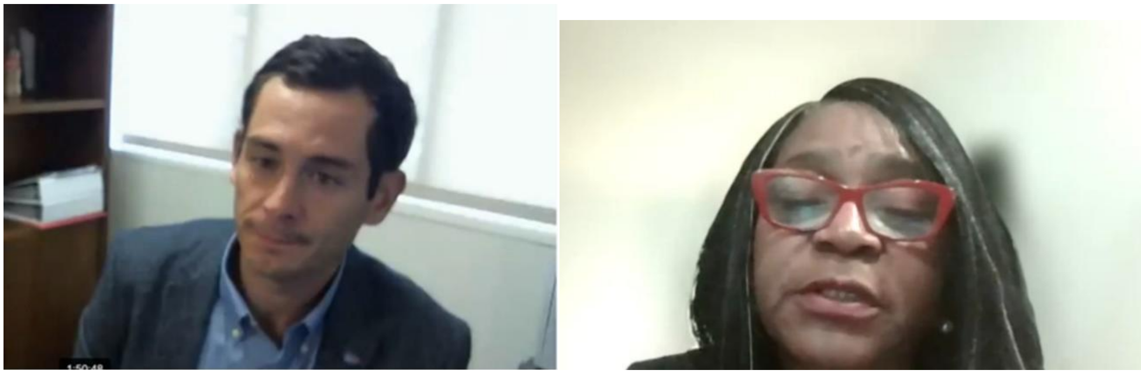
Remarks from the US Mission Representative

The remarks of the Ambassador of the United States of America was presented by David Russell, the Commercial Attaché at the Embassy of the United States in Nigeria. The CEO of ABC Nigeria, Margaret Olele, introduced Mr. Russell. In the remarks, he noted the perfect timing of the event as October is also the cybersecurity awareness month in the US. He further stated that digital technology has revolutionized every aspect of our lives. The sector is expanding at an exponential rate, especially in Nigeria. As the sector expands, criminal activities such as cybercrimes and other malicious actors, identity theft, unauthorized access and hacking have also increased.

The United States of America understands that cyber security is an important component of national security and economic policy. Cybersecurity considerations must be imbibed in our laws and policy and must be our daily habits. The United States also applauded the effort of the Nigerian government to combat cybercrimes through its initiatives and regulations.

The United States also commended its partnership with Nigeria in the area of tracking cybercriminals and looks forward to strengthening this partnerships. Mr Russell noted the importance of utilizing trusted 5G equipment and software. As such, all must be done to ensure that only trustworthy companies are suppliers and part of the value chain. He stated that all must be done to make 5G available to all Nigerians.

He also thanked Nigeria for supporting the successful bid of Doreen Dodgan-Martin to become the Secretary-General of the International Telecommunication Union. **He highly commended the ABC leadership for this initiative and recommended them as a key resource in the area of cybersecurity**. Mr. Rusell ended his remarks with the following quote from President Joe Biden's speech: "with respect to cybersecurity, vigilance and urgency today can prevent or mitigate attacks tomorrow."



L-R: David Russell and Margaret Olele, CEO of ABC, Nigeria

Remarks from the Dell Representative

Dell was one of the partners of the 2nd Cybersecurity Conference. Their representative, Mr. Mayusesh Kothari, gave a presentation on how the private sector is supporting the cyber ecosystem in Nigeria. In his presentation, Mayuresh analyzed some key steps to counter cybercrimes and cyber threats.

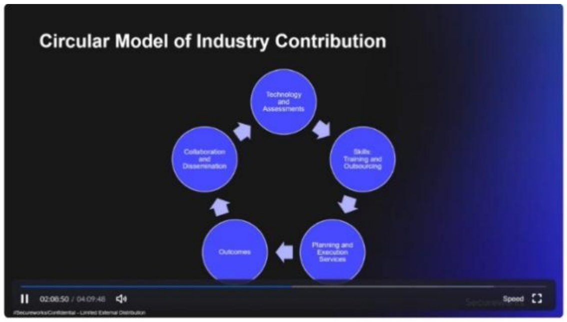
He mentioned that the first step is to identify possible targets and vulnerabilities. Next, necessary measures need to be put in place to close gaps by putting secured measures to avoid attacks using effective tools and technologies. There is also a need to develop capacity through skills training to protect cyber space. The presenter also mentioned the need to establish a process with a plan to execute, test skills with the tools and have that repeated process deployed to ensure the process is going in the right direction.

He noted that early entry into STEM careers is important but it must be balanced with an access to hands-on training and this can be provided by industry partners.

Secureworks

How Private Sector helps strengthen the Cyber Security Ecosystem

Mayuresh Kothari
Global Solution Lead
Dell Secureworks



Circular Model of Industry Contribution

Technology and Assessments
Skills Training and Outsourcing
Planning and Execution Services
Outcomes
Collaboration and Dissemination
02:08:50 / 04:09:48
Speed

Slides from the Presentation by Dell

II. Advocacy and Awareness

This panel discussed issues that promote the responsible use of cyberspace to drive Nigeria's digital economy, building trust and confidence in a safe and resilient environment and driving an elevated level of awareness on cybersecurity through associations and civil societies.

Panelists

- Dr. Bala Fakandu, Office of the National Security Adviser (ONSA);
- Prof. Adesina Sodiya, President, Nigeria Computer Society;
- Prof Olawale Ajai Lagos Business School (LBS);
- John Edokpolo, Director of Corporate, External and Legal Affairs, Microsoft, MEA Emerging Markets;
- Moderator – Mosa Mkhize, Covington

The President of the Nigeria Computer Society (NCS) was asked *about how his organization is creating awareness about cybercrimes and how they are encouraging people to pursue a career in cybersecurity*. To this question, Prof Sodiya stated that NCS has organized and will keep organizing a number of programs and activities to educate Nigerians on the threat of cybercrime, as well as the many opportunities available in the cyber ecosystem within and outside Nigeria. These programs and initiatives are implemented in partnership with the private sector and other stakeholders.

Microsoft's global online platform has experienced different kinds of threats, being a platform of choice for many businesses. The Director of Microsoft's Corporate, External and Legal Affairs was asked *how Microsoft is addressing issues related to online threats posed to vulnerable groups such as women and children*. He was also asked to *share some of the strategies used to tackle such issues*.

In his response, Mr. John Edokpolo explained that as part of the cost of going digital for work, learning and business and delivery of citizen services, there has been a proliferation of cybercrime and threats. As such, there is a need to come up with the right policy and strategy to prevent, mitigate and disrupt these attacks. He stated that Microsoft security has invested in partnerships with industries, government agencies and law enforcements to come up with practices, solutions and code of practices in order to make cyber space safer for everybody.

Furthermore, he noted that Microsoft has come up with a technology called Photo DNA which detects and reports sexually exploitative images. This Photo DNA technology has been given for free to organizations that work in line with this menace on children, to use in making their work of tracking easier.

A Professor of Legal, Social and Political Environment at the Lagos Business School was asked if he feels the legal policies and guidelines for regulation are reflective on the issue of cybercrime. In his reply, Prof. Ajai Olawale stated that a lot has been done to bring together the public and private sector along with the academia but more still needs to be done to curb these threats. He noted that the academia helps with capacity building and for example, provides critical manpower through courses in cybersecurity. Prof. Olawale went on to emphasize that cyberspace is native to younger people so there is a greater need to create awareness for students lower down the line than University students. He also stated that awareness efforts should be concerted and organized.

III. Role of Skilling and Mentoring in Cybersecurity

This panel discussed issues around the importance of skilling in developing the critical mass that Nigeria needs to develop a robust response to cyber threats and to support efforts aimed at promoting and strengthening cybersecurity efforts in the country. The panel also discussed the issue of mentorship and how it ensures that experienced cybersecurity professionals support professionals with limited cybersecurity experience.

Panelists

- Kashifu Inuwa Abdullahi CCIE, Director General/Chief Executive Officer, National Information Technology Development Agency (NITDA);
- Deon Govender, Covington Expert
- Charles Murito, Google Africa Director for Government Affairs and Public Policy
- Ketebu E. Kennedy, System Administrator/Cybersecurity expert and Team Lead Darknet, Economic and Financial Crimes Commission (EFCC);
- Abubakar Isah, Director of ICT, Federal Ministry of Education;
- Abumere Igboa, Stanbic IBTC Holdings PL¢
- Moderator – Kasim Sodangi, Smile Identity

The Director of ICT at the Federal Ministry of Education was asked about the perspective of the Ministry *regarding trends that relate to cybercrimes in Nigeria*. Mr. Abubakar Isa stated that since the advent of Covid19 and with most teaching having moved to the cyber space, there has been an increase in the number of children experiencing cyber bullying and this gives the Nigerian government a lot of concern. He noted that there is a standard procedure for national education security, however not much has been done on the cyber end because there had not been such a large number of students learning on cyberspace in the past.

The Director also noted that identity theft and hacking were some of the cybercrimes reported in the past. Mr. Isah stated that the Federal Ministry of Education is currently working with partners and security agencies to see how they can tackle these problems and inculcate cyber security into the Nigerian educational curriculum at each level in a way that supports continuous learning.

Mr. Abumere Igboa, Chairperson of the Committee of Chief Information Security Officers of Nigerian Financial Institutions was asked for his take on how financial institutions in Nigeria should handle the issue of a dearth of cybersecurity professionals. Mr. Abumere stated that it comes down to the people because most banks have the technical capability to address cybersecurity issues but there is a lack of people with the right skills to use and optimize these tools and this is where continuous training comes in. He also noted that some banks have an issue with skilled personnel leaving the shores of Nigeria to where they feel more valued. He added that there is the need to work more on capacity building and on keeping them motivated to stay back in Nigeria.

Mr. Abubakar Isah of the Federal Ministry of Education further addressed the question on how to enhance partnerships in the Ministry that can further enhance the success of the initiatives of the Ministry. Mr. Isah mentioned that the Ministry currently has a partnership with Oracle where they are comparing the curriculum used to train lecturers and students. He also noted that they have a partnership with CISCO as well as partnerships with Ministries, Departments and Agencies in Nigeria, such as the National Information Technology Development Agency (NITDA) and the Nigerian Communications Commission (NCC). Some of these partnerships supported in the development of a digital literacy policy and also aim to support the development of necessary legislation.

Charles Murito, Google Africa Director for Government Affairs and Public Policy, stated that Google had formed partnerships with several African governments, including Nigeria, to support cybersecurity efforts across the continent. He noted that Google had invested in partnerships in both the public and private sectors to ensure that users of their platforms, apps and resources were safe while using their services. Mr. Murito added that these efforts are a demonstration of Google's alignment with governments, businesses, and platforms across the continent in a bid to strengthen cybersecurity efforts across the continent.

Deon Govender, of Covington, stated that deliberate policies should be developed, articulated and implemented to forestall cybersecurity incidents in Africa. He noted that policy refreshers and trainings should be conducted to enable stakeholders appreciate the importance of policy. He also added that there is a level of preparedness required to handle the challenges that may come with addressing cyberthreats, especially for public systems as these have the capacity to negatively affect public service delivery and leave societies vulnerable. He encouraged government to develop policies and work through ideas that will make users safe. He also urged stakeholders to ensure that capacity is being built to prepare stakeholders to protect society and public services online.

All other panelists agreed on the importance of skilling and mentorship to develop a thriving cyber ecosystem and to ward off cybercriminals.

IV. Recommendations

A number of recommendations were made during the conference. Some of the key recommendations are listed below:

1. There is a need for the effective adoption of the triple helix model in promoting cybersecurity in Nigeria
2. There is the need for workplace retention policies to make it easier for women and girls to pursue careers in cybersecurity and digital technologies
3. Institutions need to focus on the development of high quality content in order to create a pool of highly competent cybersecurity experts
4. There is a need for further advocacy for the amendment of the Cybercrime Act
5. There should be collaboration between law enforcement agencies with a view to promoting cybersecurity
6. Early entry into STEM careers is important but it must be balanced with a access to hands-on training and this can be provided by industry partners
7. There is an urgent need to develop the capacity of Nigerians and increase cybersecurity awareness in the country in order to reduce the incidence of cybercrime
8. There is a need to identify practical examples that can lead to a more inclusive and diverse leadership in the digital economy sector, not just with regard to policy making but also at the implementation level
9. There is a need to see more women take up roles in creating solutions, in addition to their roles as decision makers.
10. Hackathons should be encouraged for strengthening capacity in the area of cybersecurity
11. As Nigeria adopts 5G technologies, there is a need to ensure the integrity of 5G equipment and software
12. There is a strong need to encourage collaboration among stakeholders in the cyber ecosystem
13. Government is encouraged to continually come up with the right policies and strategies to prevent, mitigate and disrupt cyber attacks

14. The Nigerian government should continue to address the issue of cybersecurity and should include it in the curriculum at the primary and secondary school levels.
15. Financial institutions and other sectors of the economy are encouraged to train and incentivize competent and hardworking personnel to retain their services within those institutions
16. Public and private sector institutions were reminded of the importance of skilling and mentorship as a way to develop a thriving cyber ecosystem that is able to consistently ward off cybercriminals

Acknowledgements

The American Business Council would like to thank all those who contributed to this report and notably the numerous organizations and private sector representatives who took the time to share their insights. Our special gratitude to the Federal Ministry of Communications and Digital Economy, Nigeria, the Ministry of ICT and Innovation, Rwanda, Dell Technologies, Comercio Limited and Naijasecforce for their partnership and generous support in making the Conference the success it was.

The American Business Council is the voice of American Businesses in Nigeria and a key vehicle for expanding trade investment opportunities between Nigeria and the United States of America in the interest of its members and both countries.

Please direct inquiries to:

American Business Council
Bishop Aboyade Cole St, KPMG Tower 6th
Floor, Victoria Island, Lagos
www.abcnig.com