Report on FIRST Regional Symposium Accra, Ghana

Alisa Hotel

30 September, 2015

Hosted By AfricaCERT

Contents

1.0 BACKGROUND

The Forum of Incident Response and Security Teams (FIRST) organized the first-ever Cyber Security Symposium in Africa on the theme, "*Joining Forces to Promote Cyber Security in Africa*" on Wednesday, September 30 2015 in Accra, Ghana. The event was hosted by the Africa Computer Emergency Response Teams (AfricaCERT). In all, 12 countries participated in this historic Symposium, which brought together high profile personalities to speak to issues pertaining to cyber security, with particular reference to Africa. The symposium was opened by the Mr. Ato Sarpong, the Deputy Minister of Communications of the Republic of Ghana.

2.0 OPENING CEREMONY

MODERATOR: Eric Akumiah, CERT-GH

Five addresses/statements were made during the Opening Ceremony. Mr. Ato Sarpong, Ghana's Deputy Minister of Communication gave the keynote address.

2.1: Remarks from AfricaCERT

Jean-Robert Hountomey, Executive Director of AfricaCERT highlighted the following:

- The importance of addressing cyber-related challenges.
- The Importance of building capacity to deal with cyber security issues.

2.2: Remarks from FIRST.org

Koichiro 'Sparky' Komiyama, a board member of FIRST represented FIRST at the opening ceremony. His speech highlighted the following:

- Inaugural FIRST regional symposium in Africa organized in collaboration with AfricaCERT to promote the platform on cyber security in Africa to share information on vulnerability, incidence and technical issues is historic and the beginning of a strong partnership.

- Africa is eager to learn and quickly develop skills in the area of cyber security.
- Africa ICT and cyber security has great potential for growth.
    - Partners are available to support the African community to build capacity
    - Since the Internet has no borders, cyber security in Africa's should be everyone's concern.
    - FIRST is new to Africa and glad to establish a mutual relationship. Currently, FIRST has 330 members in more than 75 countries.

2.3: Remarks from International Telecommunications Union (ITU)

The representative from ITU, Serge Valery Zongo of the ITU Africa regional Office in Cameroun, made the following remarks:

- Promotion of cyber security is close to the heart of the ITU
- Cyber security is crucial for the Internet to remain credible
- Importance of establishing a task force of partners and all stakeholders working together ensure cyber security in Africa.
- ITU is fully engaged with global leaders and committed to promoting cyber security.
- ITU has signed a MoU with ECOWAS and will do same with AfricaCERT on cyber security.
- Partnership is key to make cyber safe to enjoy the benefits of the Internet.

2.4: Remarks from National Communications Authority (NCA), Ghana

The representative from NCA, Albert Enninful, Deputy Director General, made the following remarks:

- Cyber security is critical because of the ever-increasing connectivity (Internet of Things, Cloud Computing etc.).
- Within the same space there are great opportunities for business, academia entertainment and enhanced living.
- It behooves on all users to change attitudes towards keeping safe to prevent cyber attacks, as every user is vulnerable.
- Capacity building is important to ensure safety in cyber space.

2.5: Remarks from Chairman of AfricaCERT Council of Elders

The Chairman of AfricaCERT Council of Elders, Prof Nii Narku Quaynor, made the following remarks:

- AfricaCERT is a platform made up of several African countries and regional collaborations that seek to bring issues bordering on the Internet for discussion.
- The gathering of stakeholders initiated by FIRST and AfricaCERT to discuss issues pertaining to cyber security is a step in the right direction and looking forward to more of such meetings
- AfricaCERT is the first African organization to join forces to promote cyber security in the region.
- The organization uses the bottom-up-approach in its operations.

2.6: Keynote Address by Hon. Ato Sarpong, Ghana's Deputy Minister for Communication

The Deputy Minister made the following remarks in his keynote address:

- Need to make our cyber space safe.
- Rapid growth of the use of the internet make us vulnerable
- Commended organizers for initiating the coming together of stakeholders
- Reference was made to the recent attacks on government website in Ghana.
- Need to build capacity as a nation to handle cyber issues and therefore more resources should be invested in the area of ICT.
- Need to bridge digital divide between the urban and rural
- Mentioned some of Ghana government's ICT initiatives.
- Government to approve the cyber security strategy by November 2015.

3.0 CYBERSECURITY ON-GOING ACTIVITIES IN AFRICA

MODERATOR: Professor Nii Quaynor

Activities of FIRST and ITU were captured in this session.

3.1 FIRST Presentation

FIRST highlighted its role in Africa, which included capacity building, as well as other opportunities open to individuals and organizations that would like to be part of the organization.

3.2 ITU Presentation

The ITU presentation spelt out some challenges in Africa concerning the ICT services uptake for African countries. On the preparedness to be part of FIRST activities, ITU intimated that there is the need to bridge the online presence in developing countries. Other challenges include the lack of:

- A legal regional framework
- Appropriate national and global organizational structures
- Skills set
- International cooperation between industry and the law enforcement agencies, regulators, academia to address these challenges.

ITU Activities in Africa

Mention was made of the global cyber agenda, legal measures, technical and procedural issues, including initiating the global cyber security index, which saw some top performing African countries emerging in their fight/preparedness in cyber security. The ITU has also prepared cyber wellness country profiles which can be searched for on their website.

Other initiatives include the following

- The child online protection policy.
- The MoU with ECOWAS to enhance cyber security profile of ECOWAS through certain initiatives.

- Enhancing cyber security in some of the least developed countries in the world, including the Gambia, Sierra Leone, and Mauritania.
- Building global partnerships with ISOC, Interpol, Symantec, Trend, ECOWAS, etc., as well as collaborating with FIRST.

As far as the ITU is concerned, a multi-stakeholder and collaborative approach is critical to deal with cyber security.

Way Forward for ITU

On the way forward, ITU said it will continue to run the following:

- CERT project
- Child online policy
- Organise fora and seminars
- Collaborate with FIRST

3.3: QA & Comments:

During the questions and answer time, some questions asked included:

- To the ITU
  - Why AfricaCERT was conspicuously missing in ITU's collaboration?
  - Lack of human resource capacity and collaboration with educational institutions to build capacity
  - The ITU academy has two Centers of Excellence in Africa, with the view to helping countries build national capacity. Participants questioned the criteria for forming centers of excellence and wanted to know why all the two centers were in Francophone Africa. In response, ITU said the centers utilize both English and French as the medium of instruction for capacity building. It was suggested that the ITU approach the Association of African Universities (AAU), Ghanaian Academic and Research Network (GarNET) and other National Research Networks (NNRENs) to take a more holistic look at issues concerning research and academia.

- To FIRST.org,
    - it was indicated that AfricaCERT and African CSIRTs should travel to the global North to attend conferences and this makes it expensive for members in Africa. There is therefore the need to look at a more realistic ways of creating platforms for both parties to meet.

4.0 CHALLENGES AND LESSONS LEARNT

MODERATOR: Prof. Nabil Sahli, TunCERT, AfricaCERT

In this session some selected CERTs in Africa, including Ghana made presentations on their CERTS and challenges they are facing in implementing their CERTs. CERT-CC and CERT-FR joined the panel to share best practices around the world.

4.1: EGYPT:

The following are some of the issues that came up in the presentation from Egypt:

- Need to for a vision and be well informed on cyber security issues and updated on globally incidences.
- Difficulties encountered include, leadership's backing on a national cyber security strategy.
- The National Telecommunication authority is in charge of cyber security.
- Lack of skills set making recruitment of staff difficult
- Ability to communicate with other entities within the constituency i.e. Government, ISPs and mobile operators
- Lack of cyber security culture
- Need to spread awareness on cyber security among stakeholders

4.2: LIBYA

The following are some of the issues that came up in the presentation from Libya:

- Challenges experienced included:
    - Poor cyber security culture
    - Lack of skills set
    - Absence of political will and stability
    - Lack of funds
- Solutions crafted to mitigate the challenges included:
    - Awareness creative on the issues

    - The institution of Kareem initiative - a mentorship programme targeting university students
    - Develop open source tools
    - Review policy and initiate a vulnerably assessment
    - Drafted the Electronic Transactions Law & Vulnerability Assessment Partnership Agreement
- Way Forward
    - CERT to be fully operational and will join FIRST
    - CERT to come out with an African cyber security guide to avoid biased information on Africa

4.3: La Cote D'Ivoire

- Factors that promote cybercrime include:
    - The lack of a legal framework
- Strategies adopted include:
    - Institution of a legal framework
    - Developed organizational structures
    - Evaluated different CERTS in the country to stir up activities of the national CERT
- Problems & challenges and solutions
    - Lack of funding for national CERT
    - Lack of involvement of relevant stakeholders
    - Lack of research, therefore need to collaborate with academia on research opportunities
    - Lack of standardized software
- Way Forward
    - Need for a database on people with skills sets

4.4: EITHIOPIA CERT & GHANA CERT

Both Ethiopia CERT and Ghana CERT shared their experiences and challenges. The problems were no different from the other CERTs preceding their presentations, citing issues such as lack of standard, lack of skillset and funding as some of the problems facing their CERTs

4.5: Q& A and comments

During the Q & A session, a number of questions were raised including the following:

- How are funds raised for CERTs? For CERTs to get funds to operate there is the need for adequate laws to be formulated to guide the CERTs
- Use of open source. How can we be sure that these tools are genuine?
- How can countries that have just started their CERTs be supported?

5.0 RESILENT E- DEVELOPMENT

MODERATOR: Professor Nii Quaynor

In this session some selected CERTs in Africa, including Ghana made presentations on their CERTS and the challenges they face in the implementation of their CERTs. CERT CC and CERT-FR joined the panel to share best practice around the world.

5.1: Cyber GREEN- Toward Healthy Cyberspace

By Koichiro 'Sparky' Komiyama, JPCERT/CC

- Shared Experience of JPCERT's Cyber Green Initiative (CGI) He said it was like Applying public healthcare model to cyber space (e.g. malaria). He said a CGI platform has been setup to determine cyber health of any network

5.2: Joined Forces to Maintain Cybersecurity in the Netherlands

By Wim Biemolt, SURFnet.

- Shared experience in the Netherlands and recommended the need for emerging CERTs to reach out to contacts globally for support to build strong and resilient CERTs.

5.3: Internet Resilience: DNSSEC deployment

By Yaovi Atohoun, ICANN.

- Shared ICANN's Roadshow experience and how the DNS security extensions function. According to ICANN Africa, out of 56 ccTLD, in the Africa Region, only 13 had signed their DNS zones. He mentioned the need to work to bring more security at the CCTLD level, to improve the lack of confidence in the CCLTDs among countries.

5.4: Collective Responsibility for Security and Resilience of the Global Routing System

By Michuki Mwangi, Internet Society, Africa Bureau

- He mention how challenges such as BGP trust, prefix hijack route leak impacted users who become stranded and are unable to have access to the Internet. He recommended that Internet Services Providers (ISPs) observe good practices so that they will not be at risks. He gave examples of resources for filtering, anti spoofs (mannrs.org) that one could subscribe to.

5.5: QA and comments

- During questions and answer time, Jaap van Ginkel, University of Amsterdam/SURFnet threw more light on Large Scale cyber security exercise they undertake in the Netherlands.

6.0 CYBERCRIME, CRITICAL INFRASTRUCTURE PROTECTION & ENFORCEMENT

MODERATOR: Col. Gbevlo Lartey

6.1: Panel Discussion on Cybercrime

The last session which was chaired by former National Security Advisor, Col. Dovlo Lartey of Ghana, comprised a panel with the following Ghanaian personalities: Lawyer George Nelson of National Security, Albert Antwi-Bosiako of e-crime (Private Sector) and C. K. Bruce of ISACA (Professional Association). The session was a very lively session articulating the changing nature of cyberspace, Ghana's experience and the need for a framework for governance in cyberspace to help fight cybercrime. Below are some of the issues that came up.

- Important to protect and enforce laws to protect cyber space as cybercrime is pervasive. This threat is a global phenomenon that affects everybody. It is importance for stakeholders to collectively discuss measures to mitigate any imminent disaster in the context of the prevailing laws.
- It is crucial to be mindful of the downsides of the Internet with its attendant vulnerabilities and threats, therefore, the need to promulgate laws to support the work of the technical people. Even though Ghana has criminal laws to protect its citizens, there are no laws to protect infrastructure.
- In addition, there are not ties between the law enforcement agencies and the private sector on cyber security.
- There is the need to promulgate laws to strengthen cyberspace in Ghana.
- All legal entities, e.g. the judiciary, Parliament, MDAs, ICANN, Interpol are all collaborating to fight cybercrime
- The private sector are, including Internet Service Providers (ISPs) are all active players in the fight against cybercrime.
- For private sector to be active, the following are needed.
    - Capacity building
    - Institutional capacity building i.e. of the judiciary

    - Criminal investigators
    - Police
    - Information sharing
    - Innovation and best practice
    - Joint technical initiatives
    - Capacity building
    - Awareness creation
- Need to obtain support from Senior Management to buy into the culture of cyber security consciousness so that they can readily put aside budgets to make set up robust Information Security Management Systems (ISMS)
- National security to anticipate cybercrime to be a step ahead of the cybercriminals.
- Need for cooperation among stakeholders
- Protection of critical infrastructure
- Creation of appropriate protocols so that we are not be found wanting e.g./ in the health and power sectors
- Local building of capacity
- Sensitization for key stakeholders on the issues

6.2: QA & Comments

The following Questions were raised:

- How can Ghana leverage to get quick response to security issues?
- How do we become competitive?
- What can we do locally to be competitive?
- In the post Snowden era, tension is mounting as some countries want a closed Internet,
- What will be the impact on the data localization on the Internet
- Need to bring nontechnical people on board who are communicators, build their capacity on the issues, so that they can repackage the information and create awareness to the general public.
- Rather than preventing a free Internet, the way forward would be to lobby for a platform for the creation of local content.

- Looking at how advanced the Internet has got too, it would not be in our interest to clamp down on its free nature as this would not inure to our benefit.
- We need to be working towards ensuring that we make the internet safe
- Awareness creation
- Bridging the legal gaps
- Enforcing the law
- Private sector participation

7.0 CLOSING REMARKS & OUTCOME

At the end of the symposium, there was an open forum for discussions, where participants gave recommendations on how to improve upon future meetings. The symposium organizers promised to make efforts to host another symposium in the region in the following year. The following were feedback from this session:

- There was an open invitation for all CERTs to join the FIRST community.
- There was a unanimous agreement by all that the symposium was very useful, bringing together all shareholders and the need to continue to build and expand the community through networking.
- The need for capacity building was reiterated.
- AfricaCERT was to help prepare next symposium.
- General call on all to collaborate to ensure a safe internet.