2017 IGF Best Practice Forum on Cybersecurity

Dear National and Regional IGF representatives,

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2017 effort. We are very interested in understanding national and regional specifics on the cybersecurity challenges we all face, and are looking for your assistance.

During 2015 and 2016, the Policy Options for Connecting and Enabling the Next Billion(s) (CENB) activity within the Internet Governance Forum identified two major elements:

- Which policy options are effective at creating an enabling environment, including deploying infrastructure, increasing usability, enabling users and ensuring affordability;
- How Connecting and Enabling the Next Billion(s) contributes to reaching the new Sustainable Development Goals (SDGs).

The Best Practice Forum on Cybersecurity realizes that making Internet access more universal, and thus it supporting the SDGs, has significant cybersecurity implications. Well-developed cybersecurity helps contribute to meeting the SDGs. Poor cybersecurity can reduce the effectiveness of these technologies, and thus limit our opportunities to helping achieve the SDGs. In our 2017 effort, we aim to identify policy mitigations that can help ensure the next billion(s) of users can be connected in a safe and reliable manner.

BPF members have already performed some security focused analysis of the CENB Phase I and II documents developed during previous years. You can review these documents here:

Security focused reading of CENB Phase I - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/687
Security focused analysis of CENB Phase II - https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/688

You can assist in the BPF by sending us answers to any or all of the following questions. They are divided in two sets:

- *General questions* should be relatively easy to answer, and provide a strong contribution to the BPF. Thank you in advance for addressing these.
- *Specific questions* are focused on very specific areas of interest. We do not expect you to respond to all of them, but if you have the opportunity to discuss them in your NRI, we welcome your input.

You are invited to share your responses on the BPF mailing list (*https://www.intgovforum.org/mailman/listinfo/bp_cybersec_2016_intgovforum.org*). For any questions, you can reach out to the Secretaria at igf@unog.ch with in cc lead expert Mr. Maarten van Horenbeeck (maarten@first.org), and the BPF's co-facilitators, Mr. Olusegun Olugbile (solugbile@gmail.com) and Mr. Markus Kummer (kummer.markus@gmail.com).

Thank you,

Markus Kummer
Olusegun Olugbile
IGF BPF on Cybersecurity co-facilitators

Questionnaire

Full Name of the NRI you are responding for: *Caribbean Internet Governance Forum (CIGF)*

Your name and official role at the NRI you are responding for:

X Coordinator
❏ Chair or co chair
❏ Member of the Steering Group/Organizing Committee/MAG of the NRI [describe which]
❏ Interested participant/observer in an NRI
❏ An NRI community member
❏ Observer on the NRIs mailing list

Your contact information (e-mail): *nigel.cassimire@ctu.int*

General questions

- Has your NRI organized a session on cybersecurity? Was it considered a priority session?
  Several sessions on cybersecurity have been organised over the years. Cybersecurity was identified as a priority topic from our first forum held in 2005. Our 4th Forum in 2008 had our first session on CSIRTs, led by a Brazilian expert.
- For how many years has your NRI covered cybersecurity as a topic?
  Since 2005. The issue was highlighted to Caribbean ICT Ministers at a briefing in 2007 and the first specialised CIGF session on cybersecurity addressed CSIRTs in 2008.
- What did the session address, or was covered in the session agenda? Were any implementation plans or policy proposals presented or discussed at your meetings, or discussed during intersessional work?
  2008: CSIRTs
  2009: CSIRTs; protecting minors online; Caribbean Internet Governance Policy Framework included policy guidelines and recommendations re cybersecurity
  2010: CSIRTs; protecting minors online; technology and secure transactions; RPKI;
  2011: Full theme on cybersecurity; partnered with OAS, ICANN and Commonwealth Secretariat; intersessional special cybersecurity /cybercrime Ministerial Seminar involving Justice Ministers and Judiciary
  2012: Intersessional Caribbean Stakeholders' Meeting (CSM) on cybersecurity developed a draft Caribbean cybersecurity framework – priorities, recommendations and timeframe; CIGF accepted policy imperatives, addressed DNSSEC and securing digital assets; Updated cybersecurity policy recommendations in the Caribbean Internet Governance Policy Framework
  2013: 3-day cybersecurity track at CIGF addressing hardware security, CSIRTs, online banking, malware, policy approaches, cybercrime trends
  2014: CIGF session addressed cybersecurity, security vs privacy, spam
  2015: CIGF addressed cybersecurity vs privacy and user rights
  2016: Intersessional CSM II developed Caribbean cybersecurity and cybercrime action plan; CIGF addressed cybersecurity and privacy issues in IoT applications; data protection regimes and best practices
  2017: Intersessional CSM III reviewed progress of Caribbean cybersecurity action plan; CIGF addressed cybersecurity threats, risks and protective measures; DNSSEC
- What were the main outcomes, or work initiated out of this session?
  Policy guidelines and recommendations re cybersecurity and cybercrime in the Caribbean Internet Governance Policy Framework; Completed a Caribbean (CARICOM)

Cybersecurity and Cybercrime Action Plan; ongoing productive collaborations among the CTU, OAS, Commonwealth organisations, Caribbean (CARICOM) organisations and the Internet technical community on cybersecurity and cybercrime policy and regulatory action

- Does your NRI maintain any key messages on cybersecurity?
  Not formally beyond the documents already produced; it is just highlighted as an ongoing priority for consistent management action.

Specific questions

- What working definition do you maintain for cybersecurity? What is considered a cybersecurity issue and what is not?
  No specific definition is maintained. A distinction is however made between cybersecurity and cybercrime, the former addressing more preventive technical, technological and administrative control issues, actions and safeguards while the latter addresses more legislative, law enforcing and judicial aspects.
- How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?
  Good cybersecurity would facilitate more growth in users and usage of internet technologies, accelerating business, growing economies and making more wealth available for distribution to support attainment of the SDGs.
- How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?
  Conversely, poor cybersecurity would tend to hinder growth in the number of users of Internet technologies, retarding usage growth and limiting the impact of ICTs on economic growth and wealth creation for attainment of the SDGs.
- Assessment of the CENB Phase II policy recommendations identified a few clear threats. Which of the following do you consider priorities? Do you see particular policy options or best practices to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:

  - Issues that impact the reliability and access to Internet services
    Priority? Yes/No - *Yes*
    Policy options?

        - *Technical measures to enhance resiliency of network access and access to services e.g. diversity of access, reliability/availability standards*
        - *Technical and administrative measures to facilitate prevention, detection and mitigation of cyber attacks and identification of perpetrators*

- Security of mobile devices
  Priority? Yes/No - *Yes*
  Policy options?
    - *Minimum built-in security features and capabilities*
    -

- Potential abuse by authorities, including surveillance
  Priority? Yes/No – *No, not identified as a major issue in this jurisdiction*
  Policy options?
    - *Legislative and constitutional safeguards*
    - *Regulatory provisions*

- Confidentiality and availability of sensitive information
  Priority? Yes/No – *Yes*
  Policy options?
    - *Data protection laws and regulatory regime*
    -

- Online abuse and gender based violence
  Priority? Yes/No - *Yes*
  Policy options?
    - *Awareness building and education programmes*
    - *State and NGO support resources*

- Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Points (IXP)
  Priority? Yes/No - *Yes*
  Policy options?
    - *DNSSEC adoption*

    - *ccTLD capacity building*
    - *IXP services and resiliency development*

- Vulnerabilities in the technologies supporting critical industrial processes such as electricity provisioning
  Priority? Yes/No - *Yes*
  Policy options?
    - *Disaster preparedness and response plans*
    - *Business continuity plans*
    -

- De-anonymization of improperly anonymized citizen data
  Priority? Yes/No – *As above for confidentiality and availability of sensitive information*
  Policy options?
    -
    -

- The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis
  Priority? Yes/No – *Not identified*
  Policy options?
    -
    -

- Internet of Things security.
  Priority? Yes/No - *Yes*
  Policy options?
    - *Still under development*
    -

- Human Factors and security awareness and education
  Priority? Yes/No - *Yes*
  Policy options?
    - *Specific measures still under development*
    -

- ○ **Other**: describe a cybersecurity issue critical to developing the SDGs in relevant to your nation or region (100 words or less)
  Priority? Yes/No
  Policy options?

    - *Educating users (the general public) to become more aware of how to recognise possible suspicious activity and attacks and how to effectively avoid them or deal with them. This, of course, is a moving target as the attack techniques are constantly evolving.*
    -

- Please, enumerate Innovative Practices in the field of cybersecurity that you have seen discussed in your community, and which help promote the safe connection of the next billion(s) of users, or promote the Sustainable Development Goals.
    - *Collaboration and information sharing among stakeholders for example through the formation and proceedings of the Caribbean Network Operators Group (CaribNOG) in the technical community and, at the policy level, the multi-stakeholder Caribbean ICT Collaboration Committee.*

- Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity.

  This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

- Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

    - *In fostering open inter-stakeholder collaboration and trust relationships*
    - *In infusing a culture of cybersecurity among all stakeholder groups given the irreversible and cross-cutting impact of the Internet on all aspects of economic and social life.*

- What is for you the most critical cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?
    - *Fostering the appropriate culture of cybersecurity appropriate to each stakeholder group e.g. policy makers, technical community, service providers, end users. Each stakeholder group has to be addressed.*
- How about bringing an awareness about Cyber Security Intelligence and its potentiality?
    - *Yes, but this might be more relevant to the technical community.*