IGF 2017 Workshop Report: WS100

Session Title:
Bridging digital divides through cybersecurity capacity building

Date:
19 December 2017

Time:
11:50-13:20

Session Organizer:
International Chamber of Commerce Business Action to Support the Information Society (ICC BASIS)
Global Cyber Security Capacity Centre, University of Oxford
Organisation of American States

Chair/Moderator:
Dominique Lazanski, GSMA

Rapporteur/Notetaker:
Stephanie MacLellan, CIGI

List of Speakers and their institutional affiliations:
- Belisario Contreras, Organization of American States
- Sadie Creese, Global Cyber Security Capacity Centre, University of Oxford
- Carmen Gonsalves, Netherlands Government
- Lillian Nalwoga, ISOC Uganda
- Audrey Plonk, Intel

Key Issues raised (1 sentence per issue):
Trust: Security is crucial for new internet users to develop trust in the system, which will encourage them to keep using the internet – thus building capacity and spreading the benefits of digitization.

Local context: Cybersecurity capacity-building initiatives must account for the social, economic and cultural environments of the country/region, and include consultation to take advantage of regional and local expertise and relationships.

Multistakeholderism: A multistakeholder approach to cybersecurity capacity-building allows for input from various perspectives, which is essential when so many systems are highly integrated and affect multiple sectors. This also allows for the sharing of good practices.

Education and training: Education and training should be seen as part of any capacity-building initiative, both inside government institutions and in classrooms at all educational levels.

Digital divide: Cybersecurity capacity-building should be seen as a way to bridge the digital divide and allow the benefits of digitization to reach less connected, developing countries.

Awareness: Lack of awareness can be a barrier to capacity building: if governments, civil society groups and other sectors aren't aware of the risks and lost opportunities a country faces with a limited cybersecurity capacity, they won't invest in capacity building.

If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

Lillian Nalwoga summarized the relationship between internet access, security and trust, drawing on her experience in the African context, where the proportion of the population that has access to the Internet is far lower than the global average. She said that when new users first connect to the internet, they need to see that it is secure and functional in order to develop trust in the system, which will encourage them to keep using the Internet and build capacity. For instance, if their financial information is secure when they use electronic payments or e-commerce sites, this can help grow the local digital economy.

Belisario Contreras noted that capacity building must focus not just on the institutions involved, but recognize that the institutions are made up of the human beings who work there. As part of this, capacity-building efforts must recognize the local context in order to be effective, with initiatives that are tailored to account for the social, economic and cultural environments of the country/region. But regardless of the local environment, basic human rights principles should remain consistent, such as freedom of speech, privacy, gender inclusivity and diversity.

Audrey Plonk contributed a private-sector perspective. She said that when companies develop products, they need to work with people "on the other side," such as governments, civil society and other companies, to help confront issues that arise. This is particularly important because systems are highly integrated, which means security issues often affect more than one company. She also spoke of the importance of cybersecurity education and training, saying this should be integrated into the education system at all levels, from elementary schools to universities, and that cybersecurity should be treated as a component of the discipline of computer science rather than a separate field.

Sadie Creese described the Cybersecurity Capacity Maturity Model that has been developed by the Global Cybersecurity Capacity Centre. This model helps countries assess their maturity and capacity when it comes to setting policy, developing laws and regulations, setting standards, developing education and leadership, etc. The model was designed in partnership with stakeholders from various sectors around the world, and the centre uses a multistakeholder approach when deploying the model – eg. by working with focus groups to reach a consensus on what the local capacity is and how to grow it. The centre also works with international organizations, such as the OAS and the World Bank, so those organizations can use the model to help assess the needs of the countries where they work.

Carmen Gonsalves spoke about the Global Forum for Cyber Expertise, which was established in 2015 to share best practices and successful policies among stakeholdes from multiple sectors. It now has 60 members, including states, international organizations and private sector representatives, and it works closely with civil society. In the course of its work, the forum came to view cybersecurity capacity building as important not just for its own sake, but as a precondition for bridging the digital divide and spreading the benefits of digitization.

Please describe the Discussions that took place during the workshop session (3 paragraphs):

The participants divided into three breakout discussion groups and reported back to share a summary of their discussions. The breakout groups were highly engaged in the discussions and Plonk observed that "there was much more willingness to share than we may have expected."

Group 1 said there was a need for more research on existing cybersecurity programs and their effectiveness in order to help governments decide how to allocate their resources when it comes to building capacity. They also called for more research to show the effectiveness of cyber education in improving security and bridging the digital divide.

Group 2 suggested that awareness-raising could contribute to capacity building, because greater awareness among governments about cyber risks could encourage them to invest more in capacity building. They also saw the potential for regional support to help countries build their capacity and follow international standards and norms.

Group 3 also spoke of a lack of awareness about cybersecurity issues. For example, security is sometimes seen as a luxury of secondary importance to expanding internet access, when they should be pursued concurrently. In other situations, too much focus on cyber risk can be a deterrent to expanding internet access. In addition to awareness, a lack of resources – both financial and expertise – is a major barrier to capacity building. They also spoke of the need for a common understanding of relevant concepts that can be globally applicable, but also flexible enough to adapt to local needs.

Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):
See above

Gender Reporting

- Estimate the overall number of the participants present at the session: 50

- Estimate the overall number of women present at the session: 45% (5/6 panelists were women)

- To what extent did the session discuss gender equality and/or women's empowerment?
It was addressed in passing in the speakers' comments but was not a focus of the discussion.

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:
Contreras included gender inclusivity among a number of basic human rights principles (such as freedom of speech, privacy and diversity) that must be considered when it comes to capacity building.