Summary of the informal BPF Cybersecurity coordination session at IGF 2017

Cybersecurity BPF Coordination Session

Thursday, December 21st from 13:30 to 15:00

Room XXVII - E United Nations Office at Geneva (UNOG)

Summary

This session was organized as an outcome of our final Best Practices Forum (BPF) call ahead of the IGF. Several parties expressed an interest in having an informal session to discuss the work of the BPF, rather than simply the subject matter. In particular, we wanted to have an exchange of ideas on where to take the BPF in future years.

During the session, we discussed how the BPF contributes to wider IGF goals by creating a multistakeholder space to collect best practices and experiences around cybersecurity from a wide variety of stakeholders, including by leveraging the National and Regional IGF communities.

This discussion helps build a common understanding between all parties involved, creates an opportunity to exchange views on areas where no consensus exists, and creates a space for learning about topics that are not yet at a level of shared understanding. In addition, the BPF has provided an opportunity to build on previous work within the BPF community, such as the Connecting and Enabling the Next Billion (CENB) work.

In the session, we learned from several government representatives that in order to improve government participation, we would benefit from collecting best practices which everyone should apply, but which may not be universally known or shared. While it was understood that cybersecurity included sensitive issues governments would not be ready to address in an open setting, the representatives of Israel and Switzerland made it clear that they found it essential to engage with non-governmental stakeholders. n addition we should consider leveling up the conversation to a point where the stakes of not participating are higher.

Agenda

This session was organized at the end of the IGF with two main agenda items:

- What issues should be addressed by the broader IGF community?
- What are our priorities for 2018, should the BPF be renewed?
- Looking back at 2017, what worked well? What did not?

The session took place as an additional session, with no transcription, though remote participation was supported and available. A video recording is available at https://youtu.be/owEP5G9hz4E .

The session took place in addition to the main BPF on Cybersecurity session, which was recorded and made available here. A transcript of the main session is available here.

Discussion

Follow up on items from the main BPF meeting

● The session was opened with a comment by David Rufenacht on the current draft document regarding medical devices. Medical devices are sometimes sold on hardware which is only certificate to work with Windows XP, even though that operating system itself is no longer supported. The misalignment between these life-cycles can cause significant security issues, as security updates may no longer be available for the only supported combination. It was suggested this would be a great illustration for the importance of managing a product lifecycle, currently included as a recommendation in the 2017 draft document.

<u>What went well, what did not go very well</u>

● Markus Kummer noted the solid discussion which took place throughout the year. He also noted the draft version of the BPF outcome document is still available for public comment. He also stated that renewal of the BPF is up to the Multistakeholder Advisory Group, but that as a group we can propose a set of issues and themes as paths forward for consideration.

● Maarten Van Horenbeeck noted that this year we had two major challenges we identified:

○ While we hit the ground running generating a proposal for 2017 work, renewal of the group took place in April, so formal work only got started around that time;

○ We saw limited participation from private sector and government.

● Some discussion took place on what makes the IGF a valuable place for the BPF to take place in. The IGF enables countries to move forward, share thoughts and promote better understanding. The BPF in particular promotes global interoperability, creates interfaces for conversation and enables us to develop agreement on limited areas of difference.

● Markus Kummer noted that the value added by the BPF is to bring stakeholders together in an area where they can develop a common understanding, and under one roof, regardless of their background as a stakeholder community.

● Adli Wahid of APNIC noted that there is an opportunity to improve in a few ways:

○ We can engage more closely with the National and Regional IGFs, to increase the input and participation from these communities.

○ The logistical side of this year's IGF made it more difficult to have widespread participation due to the room layouts.

● Markus Kummer and Maarten Van Horenbeeck noted that some outreach had taken place this year to the NRIs, and that there is definitely room for improvement through direct outreach to their meetings. There are also potential opportunities to improve cooperation in the meeting room facilities through the use of electronic queuing mechanisms, though as the location changes from year to year, meeting room use may be different in future years.

● Sivasubramanian Muthusamy noted how the Best Practices Forum must continue to be multi-stakeholder, and is one of only a few opportunities for cybersecurity to be discussed in a public forum. Governments may not always be comfortable discussing cybersecurity in such a public space.

● Paul Wilson of APNIC noted that security has skyrocketed as a concern, including in the Regional Internet Registries. He hopes the Best Practices Forum will continue. Over the last few years he has seen the tone on cybersecurity at the IGF change, from being developmental to being more fear-focused. He sees more space for discussion within the IGF community, and sees potential opportunities for the BPF to help resolve duplication, for instance by creating interconnection with other forums such as the GFCE, which are also working on development and capacity building.

● Markus Kummer noted that the BPF is not a trade-off between security and openness, but that we need to find ways for both to contribute to eachother.

- Winston Roberts, in this forum representing an NGO, but formerly a government representative, noted that governments are often nervous about joining a forum on cybersecurity. We may need to elevate our debate and make it more applicable to their day to day work. In order to do so we'd need to pitch our discussions at a level where the stakes of not participating are clear.

- Amit Ashkenazi of the Prime Minister's Office of Israel noted that many issues are not technical, and several important security solutions are quite simple, such as the requirement to update systems to their most recent patch levels. The BPF could help identify these basic steps that provide a large portion of the value.

- David Rufenacht from MELANI noted how security is a shared responsibility. The government cannot provide it independently. For instance in his example of medical devices, a multi-stakeholder approach is a requirement to properly understand, share and address risk.

<u>Where do we take work next year?</u>

- In the earlier BPF meeting, we raised two areas of possible future development that appeared useful for further investigation:
    - ○ Defining and identifying cybersecurity culture, norms and values;
    - ○ Identifying the risk of a potential digital security divide, between those who have, and those who do not have, access to cybersecurity measures.

- Mike Nelson of Cloudflare participated remotely, noting that the rise in Distributed Denial of Service Attack is an increasing concerns. Countries are increasingly talking about standards to help address the challenge of vulnerable devices. A possible interesting avenue of communication for us could be to collect best practices on how not to build standards. Can the BPF help provide guidance on best practices moving forward on how these standards can be designed and implemented?

- Wout de Natris of de Natris Consult noted how on day 0, he organized a session on "Strengthening cooperation within the context of the IGF: Creating a roadmap for 2018". In this session he investigated what it was that made Private Sector and Government participate in IGF work. The three key reasons were:
    - ○ It fit in with their priorities of what is important work;
    - ○ There is a concrete outcome and a goal;
    - ○ The effort is focused on a single, achievable task.

Based on this, Wout recommends that our effort for future years be more focused, to gain additional traction and engagement. An example of this could be to address the risk of IoT devices by identifying a single action that should be taken, for instance, to ship any IoT device with a unique password, and then working in the BPF to drive all stakeholders to that goal. The goal should have a timeframe assigned to it, for instance "within two years".

- Mike Nelson agreed with the idea to identify best practices: what has worked, where has it worked, where has it not. He also noted that there's value in clarifying terminology - as IGF participants often talk past each other. There could be value in designing some type of taxonomy.

- It was raised in discussion that perhaps outside of trying to define a term, some education could take place on existing terminology, to avoid reinterpretation and changing already established terminology. This could perhaps even include an explanation of the history of the term: where did it come from, and what is it currently being used for -- and how did the term get there?

- Louise Marie Hurel wondered if we could take a topic, such as IoT security, and review it from a cross-cutting way, out of the perspective of each stakeholder group. What would a user-centric approach to IoT security look like, and what can our Best Practices community collect and share from this perspective? We should avoid creating a list of process issues, and coming up with a diagnosis. Instead, we can collect work that has actually contributed and made things more secure.

● Serge Droz from FIRST identified three areas of potential work:

○ He noted that taxonomies are useful to define whether something is truly a problem or not.

○ There is work to be done on our multi-stakeholder approach, to define the exact responsibilities of each group: who designs, who implements, who regulates?

○ He also sees value in noting how different best practices work in unique contexts: for instance, does a particular solution work equally effectively in Africa, or is its use restricted to e.g. EU countries? For what reason?

● Bevil Wooding of the Caribbean NOG gave an example of a project in Belize, where they brought a wide variety of stakeholders together to evaluate cybersecurity implementations. This brought a richness of discussion they had not had before. They developed individual fora for stakeholder groups, and then brought all groups together in a national cybersecurity symposium. In the symposium, they discussed "the same thing at the same time", defining areas and priorities. This then led to the development of a national cybersecurity agenda. They called the positive outcome of this process the "Belize discovery", and it is a best practice they can share.

● David Rufenacht of MELANI noted that IoT as a topic may be too large for the Best Practices Forum, and that the issue of unique passwords is also not valid in all situations: such as when managing objects instead of devices. He does agree with the idea of taking an issue and looking at it from different ways. This can help create stories and real life examples that can be put to work for others.

Other learnings and next steps

● As a next step, we will identify a small number of possible options to move forward, potentially including a cross-cutting look at a specific topic, or the idea of investigating culture, norms and values, or the digital security divide, more deeply. With the group we will start in January by identifying possible new areas of work, and making a proposal, or providing a shortlist of proposals, to the MAG for consideration.

● Wout de Natris noted that we need to do better at reiterating our successes. Things have changed because of the work in the Best Practices Forum. For instance, the BPF on CSIRT documentation was adopted as pre-reading to the GCCS 2015, and at least one CSIRT had been built using the IGF BPF on CSIRT documentation as a guide. Hence the documents we have produced has been useful, and it is important we continue to flag this.

● Anriette Esterhuysen noted she has been following the work of the BPF closely. She believes the secretariat could provide more support by reaching out to member States and making them more aware of the BPF work. However, they are most likely not sufficiently staffed. The Germans, who have shown an interest in hosting the IGF in 2019, could take a strong role in bringing these outcomes to other countries.

● Olusegun noted that we can all become ambassadors of the BPF. In 2017, he brought several Nigerian government delegates to the BPF meeting. In his view, if we bring the BPF outcome documents to Nigeria and work with them to adopt them, we can replicate that work across Western Africa. He also believes we should do more to bring the work to the core government implementers, rather than to policy analysts who may not be practically involved in cyber security.

● Maarten Van Horenbeeck and Wim Degezelle acknowledged there is a tension in terms of next steps between being inclusive of all stakeholder groups, or going more technical and diving deeper. However, that tension is healthy and shows that the group can actually work across multiple areas. Whatever decision we make in terms of progress next year, we will need to be cognizant of these conflicting interests and find a good way forward.