IGF 2024 Best Practice Forum

on

Cybersecurity Capacity Building

Main session, Tuesday 17 December, Riyadh

www.intgovforum.org/en/content/*bpf-cybersecurity*

IGF2024 Best Practice Forum on Cybersecurity Capacity Building

Welcome & session outline

Session outline

- Introduction to the Best Practice Forum, past work and overview of discussions in 2024
- Development of a problem statement
- Discussion involving expert panel and experiences from the room

Session objectives

- Discuss and refine the problem statement
- Identify answers, best practices and solutions
- Next steps ?

IGF Best Practice Forum Cybersecurity

2018 - 2023

-> IGF intersessional activity

-> different aspects of **CYBER NORMS AGREEMENTS**

- Culture, norms and values in cybersecurity (2018)
- Cybersecurity norms operationalisation (2019)
- Lessons from norms in non-cyber governance (2020)
- Drivers behind cybersecurity initiatives (2021)
- Norms elements & use of storytelling (2022)
- Cybersecurity events to inform norms deliberation (2023)

These output reports are available on the BPF's webpage at https://intgovforum.org/en/content/bpf-cybersecurity

IGF intersessional activity 2024

Best Practice Forum on Cybersecurity Capacity Building

Mainstreaming capacity building for cybersecurity, trust, and safety online

"Cybersecurity and Trust emerged as paramount concerns in the community consultation for IGF Thematic input. The topic breaks down into a complex array of issues. **This intersessional activity intends to look into capacity building to enhance cybersecurity and trust."**

- The proposal for a BPF on Cybersecurity Capacity Building as part of the 2024 cycle of IGF intersessional activities was presented and confirmed at the February meeting of the IGF Multistakeholder Advisory Group (MAG) in Riyadh.
- The BPF's work plan was subsequently presented to the broader IGF community, inviting feedback for further refinement.

Following the consultation and feedback received, the work plan was updated. Most notably, the BPF shifted its focus from compiling a mapping of existing cybersecurity capacity-building initiatives, to instead start from the observation that several organisations already provide such mappings and inventories.

It was recommended that the BPF explore how this wealth of information is available and accessible to those seeking cybersecurity capacity building, and discuss suggestions to facilitate the efficient exchange of information and ensure it effectively reaches its target audiences.

This led to the formulation of a new problem statement:

While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity-building offerings, overlaps and gaps in information exist and the information may not reach its target audience effectively.

Panel

Ms Tereza Horejsova
Ambassador Brendan Dowling
Mr João Moreno Falcão
Ms Saba Tiku Beyene

Discussion round 1: Feedback on the problem statement

Discussion round 2: How to address this?

opportunities, best practices, solutions (quick fixes, long term), recommendations

"While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity-building offerings, overlaps and gaps in information exist and the information may not reach its target audience effectively."

Session wrap up

Conclusions ?

Lessons learned ?

Recommendations ?

Suggested next steps ?

IGF 2024 BPF on Cybersecurity Capacity Building

www.intgovforum.org/en/content/bpf-cybersecurity

The BPF coordinating team:

Ms Josephine Miliza, Ms Carina Birarda, Mx Oktavía Hrund G Jóns, Ms Hariniombonana Andriamampionona, Mr Dino Cataldo Dell'Accio, Mr Wim Degezelle