IGF 2024

Best Practice Forum

Mainstreaming capacity building for cybersecurity, trust, and safety online

(BPF Cybersecurity Capacity Building)

Placeholder BPF output report

Outline

Cybersecurity and trust emerged as paramount concerns in the community consultation that was held to inform the planning and thematic focus of the IGF 2024 process and the 19th annual meeting in Riyadh. The topic breaks down into a complex array of issues, the Best Practice Forum (BPF) focussed on capacity building and fostering a culture of learning and continuous improvement to enhance cybersecurity and trust.

The BPF initially proposed to compile an overview of existing cyber-capacity building initiatives and present them in an informative database for those seeking such resources. However, when this work plan was presented to the stakeholder community, the feedback highlighted that such an effort would duplicate the work of several valuable initiatives that already map cybersecurity capacity building and provide tools to make these resources accessible. Instead, it was recommended that the BPF focus on facilitating access to the wealth of information available in mappings and inventories, ensuring it effectively reaches its target audiences.

This resulted in the formulation of a new problem statement as foundation for the BPF's work: *'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.'* Experts and stakeholders that took part in BPF discussions largely agreed that the statement is both valid and necessary but emphasized the importance of context and experience.

Consistency is essential to creating meaningful impact in capacity-building efforts. Initiatives must be rooted in local contexts while being shared globally to ensure relevance

and scalability. Localisation is pivotal to making resources accessible and fostering wider adoption. A commitment to building trust is key, achieved through actions like sharing knowledge, listening to feedback, implementing strategies, and embracing change.

Capacity-building efforts should **make full use of existing mechanisms, processes, and practices.** Existing mechanisms, including platforms such as the IGF should be utilised more effectively for capacity building activities. Cyber capacity building should be understood as an ecosystem of interconnected initiatives and practices that work together, and engagement on multiple levels, leveraging knowledge and know-how.

A participatory, multi-stakeholder approach is crucial for sustainable and inclusive cyber capacity building. Efforts should be optimized through mapping, coordinating, collaborating, and fostering dialogue, especially in low-resource environments. Cybersecurity should be demystified through accessible resources, framed as an investment in the resilience of future generations. Effective capacity-building should be consistent, localised, contextual, relevant, and well-resourced to ensure accessibility.

The recommendations outlined above are further expanded upon in the BPF Cybersecurity 2024 report.

Over the years, the BPF Cybersecurity has explored various aspects of culture, norms, and values in cybersecurity. These reports, based on insights from the IGF stakeholder community, offer valuable perspectives and are accessible on the BPF's webpage.

In previous years the BPF Cybersecurity explored different aspects of culture, norms and values in cybersecurity. These output reports are an interesting read and available on the.