IGF 2023

**Best Practice Forum Cybersecurity**

(BPF Cybersecurity)

**Lessons from cybersecurity events to inform cybersecurity policy and norms deliberations.**

---


Summary

Cybersecurity events and the experiences of first responders and those most affected provide valuable input for those involved in high-level cyber policy discussions and the development of cyber norms. At the end of the day, these policies and norms must make a difference in the lived experience of the people directly affected by or responding to incidents.

The IGF Best Practice Forum on Cybersecurity (BPF Cybersecurity) in 2021 found that the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past (IGF 2021 BPF Cybersecurity, *The use of norms to foster trust and security.*). This analysis also uncovered a missing nuance in norms and policy that could be obtained from deeper stakeholder involvement and the experiences of those most affected. As part of its activities in 2022, the BPF explored how storybanking can help to better understand events and lifting voices of those directly involved.

This year, the BPF Cybersecurty 2023, based on the previous work, evaluated cybersecurity events with the objective to present first-person experiences and narratives from those affected as victims or first responders to policy and norms developing deliberations, so that high-level policy decisions are grounded in reality. The BPF asked the community, via an open survey, what cyber incidents it is most concerned about and then selected a shortlist of events for a deeper analysis by volunteer groups. The BPF draft findings (Oct 2023) were discussed at the BPF session at the IGF 2023 annual meeting in Kyoto (12 October).

The following cases have been explored: *2022-2023 Black Axe cyber criminal activities*, *2022 ransomware incidents in Costa Rica*, *2021 Medibank incident*, *ransomware incidents in the Pacific in 2021-2023*, and the *2020 Solarwinds breach.*

Observations and trends that emerged from the analysis.

- Discussions around major cyber incidents often revolve around the technical, financial, legal, and intergovernmental consequences. However, the opportunities and challenges presented across the cyber ecosystem ultimately lie with the public, whether individuals or societies affected directly by a cyber incident or through the resonating impacts of an incident. (e.g. impact on human services, privacy and data concerns, flow-on effects and impact of cyber incidents beyond the technical or service delivery space).
- Regardless of any attributions in the cases examined, there are clear norms that could be directly applied to prevent, respond, or mitigate the impacts of the incidents explored. (e.g.

interstate cooperation on security, respect for human rights, cooperation to stop crime and terrorism, respond to requests for assistance, report ICT vulnerabilities, cyber capacity building).

- Cyber capacity building is the most prominent theme across the incidents explored, with the need for further cyber capacity building activities made clear and in many cases acted upon. More significantly however, many of the incidents explored showcased the positive impact of previous cyber capacity building activities on economies' and organisations' ability to respond to the incidents themselves. (e.g. established networks of trust and information sharing, or trainings that allowed and facilitated local teams to be able to respond).

Concluding remark

The BPF work saw early themes developing across the cases examined. It is, however, still very much a starting point for wider investigation seeking to ground discussions of international norms in real incidents and inform them on the wider impacts cyber incidents can have on the everyday lives of citizens, regardless of State or non-state involvement.

**The Report of the IGF 2023 Best Practice Forum Cybersecurity is available at** https://www.intgovforum.org/en/filedepot_download/56/26668 .