IGF 2023
Best Practice Forum Cybersecurity
(BPF Cybersecurity)

BPF Cybersecurity 2023
22 June 2023

Summary

Introduction

1. The Best Practice Forum on Cybersecurity is an IGF intersessional activity to collect existing and emerging good practices from community experience. The bottom-up developed BPF outputs intend to contribute to an understanding of global good practice, and to serve as a resource to inform policy discussions, standards development, business decisions, as well as public understanding, awareness and discourse. The work of the BPF is coordinated by a team[1] consisting of expert and MAG co-facilitators supported by the IGF Secretariat. The BPF calls and mailing list[2] are open to all interested.

2. The BPF in 2023 intends *'to collect and evaluate cybersecurity events to present first-person narratives from those most affected as victims or first responders to policy and norms developing deliberations, so that high-level policy decisions are grounded in reality.'*[3]

3. After its kick-off call, the BPF launched a survey to get a general idea of what cybersecurity incidents people are interested in and care about. The received input was pulled together in a spreadsheet that describes the various incidents, categorises them on the basis of timeframe, type of incident, geographical impact, and the impact on international stability. BPF participants were then invited to review and consolidate the list of 'incidents of interest'. This resulted in a shortlist of incidents (see next page) that was presented during the call.

[1] BPF CS 2023 coordinating team consists of Mr Klée Aiken, Mr Bart Hogeveen, Ms Sheetal Kuman (BPF Lead-experts and co-facilitator); Ms Hariniombonana Andriamampionona, Ms Carina Birarda, Ms Josephine Miliza (IGF MAG co-facilitators); Mr Wim Degezelle (BPF Cybersecurity Consultant IGF Secretariat).
[2] Subscribe to the mailing list at https://mail.intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org
[3] proposal for a BPF Cybersecurity in 2023

Shortlist of incidents of interest for BPF review - selected to be geographically diverse and diverse in type of incidents

SHORTLIST OF CYBERSECURITY INCIDENTS FOR 2023 IGF BPF ON CYBERSECURITY

Name/case	Costa Rica*	Medibank*	Ransomware Pacific*	BlackAxe*	Colonial Pipeline	Hacking democracies*
Analysis of the incident - how did the incident become known? - what happened with the incident? - what was the response by CERTs, government, and affected entities? - how was the response organised - public-private; national-international?	*Costa Rican govt agencies fell victim to a ransomware operation which caused international trade, customs operations to come to a standstill. CR declared a state of emergency, and state of war.*	*Medibank, a private health insurance company, suffered a data breach. The hackers threatened to release sensitive personal data in return for a payment. The company refused payment and data was leaked on darknet.*	*Various unrelated incidents affecting PNG Department of Finance, Tonga's Cable Communication, and Vanuatu's e-government portfolio*	*Police arrested more than 70 alleged fraudsters linked to a Nigerian criminal network known as Black Axe in South Africa, Nigeria and Ivory Coast – as well as in Europe, the Middle East, south-east Asia and the US. BlackAxe is held responsible for online scams and running digital extortion schemes.*	*The Colonial Pipeline Company halted all pipeline operations after it suffered a ransomware attack. Overseen by the FBI, the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million USD). Upon receipt of the ransom, an IT tool was provided to restore the system but it had a very long processing time to get the system back up in time.*	*Two separate incidents that affected elections or key democratic institutions. Attacks on Estonia's elections; DDoS on France's*

*It was suggested to add the SolarWinds incident to the shortlist and revisit the research that was conducted by the BPF Cybersecurity in 2022.

Next Step: Analysis of the shortlisted cybersecurity incidents - aim and methodology

4. The BPF wants to go beyond the technical aspects and the UN global normative aspects of the incidents and dig down to the impact on the stakeholders involved and make a human connection. The aim is to unpack events in such a way that makes them accessible to a broad audience and in particular a policy-makers audience.

5. For the analysis of the events, the BPF counts on volunteers. The help of people with local knowledge, including non-English language, is seen as crucial to collect stories reflecting first responder and victim perspectives, e.g. from local newspapers or other local online resources, interviews, etc. .

6. To structure the analysis it is suggested to look at the impact on 5 sectors or stakeholder groups that are enshrined in many cyber norms agreements, are of particular concern, or can rely on a certain level of protection: people, critical infrastructure/critical information infrastructure, government services, technical infrastructure, the incident's first responders. The description of each incident should then conclude with an analysis of how the incident affected international peace and stability and the relation between states.

Call for volunteers

7. Volunteers are sought to collaborate on concise descriptions of the shortlisted events, based on what is out in the public domain in terms of information, opinions, statements, anecdotal evidence, etc., and answer the following research questions:
    1) What was the impact on people?
    2) What was the impact on CI/CII?
    3) What was the impact on government services?
    4) What was the impact on technical (infra)structure?
    5) What was the impact on incident responders?
    6) How did the incident affect international peace and stability, relations between states?

8. Small groups are expected to self organise work over the next 4 to 6 weeks and compile a first draft analysis by mid August at what time a BPF call will be organised to discuss preliminary results.

Outreach and AoB

9. A request for volunteers will be sent to the BPF mailing list (a number of people already submitted their name for one of the events in response to an earlier call and during the meeting).

10. The BPF coordinating team will consider reaching out to people and organisations that may have relevant information and interested to contribute to this work, including other IGF intersessional activities and NRIs, in particular NRIs from regions where the incident had a high impact. (for example a session on ransomware incidents in the Pacific region is planned at APIGF in August).

Recording:
https://intgovforum.zoom.us/rec/share/bHWnmgTGqRoiFBKgXBEtoUIQjxZhSaccqf0hnltfsM3SoEMftJz7NTvpV5zdOk23.Uo_nBQ36tVBlh_yM?startTime=1687433076000
Passcode: &cSD1B@V

List of participants: *Aji Fama Jobe, Alembe Joseph, Alessia Sposini, Alhagie Mbow, Bart Hogeveen, Delfi Ramirez, Eduard Jacob, Iombonana Andriamampionona, John-Michael (JM) Poon, Josephine Miliza, Judith Hellerstein, June Parris, Klee Aiken, Marilee D'Arceuil, Melanie Garson, Melody Musoni, Mohamed Sylla, Néstor Boniche González, Nthabiseng Kotsokoane, Sheetal Kumar, Titti Cassa, Wim Degezelle.*