IGF 2022

Best Practice Forum Cybersecurity

Workstream 2

Exploring historic cybersecurity events

DRAFT BPF OUTPUT DOCUMENT

NOVEMBER 2022

IGF2022
Best Practice Forum Cybersecurity
Workstream 2
Exploring historic cybersecurity events

Table of contents

1. Introduction - the IGF Best Practice Forum Cybersecurity

The Internet Governance Forum, convened by the United Nations Secretary-General, is the global multistakeholder platform facilitating the discussions of public policy issues pertaining to the internet. As part of its mandate[1], the IGF facilitates the exchange of information and identifies best practices identified by experts and academics working on area issues.

Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics as a multistakeholder group. From 2018 onwards, the BPF on Cybersecurity instigated investigations of cultures of cybersecurity, identifying the norms and values in development of these practices.

As a global initiative, the IGF BPF on Cybersecurity leverages an international and cross-stakeholder approach in their operationalization of cybernorms. The BPF recognizes the significance of powerful norm promoters and of ensuring incentives as critical in global governance. They state “norm development, even without results, creates socialization, which can be critical for further success”[2].

2. Introduction to Workstream 2 - Exploring historic cybersecurity events

2.1. 2021 work and key findings

In 2021, the work stream 2 produced a report[3] that took a closer look at notable cybersecurity events of the past and wondered if norms would have made a difference, and whether these notable events led to changes in norms frameworks.

The investigators found that **the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past**. However, each analysis uncovered a missing nuance from deeper stakeholder involvement, to application of existing legal frameworks.

The differential in depth of analysis between the events with desk research only versus those for which qualitative interviews were also conducted, made clear that **the voices of those most affected by cybersecurity events provide key nuance that are not present in secondary source reports or tertiary source reporting.**

---

[1] https://www.intgovforum.org/en/about
[2] IGF 2020 BPF Cybersecurity, *Exploring best practices in relation to international cybersecurity agreements.* *https://www.intgovforum.org/en/filedepot_download/10387/2397*
[3] IGF 2021 BPF Cybersecurity, *The use of norms to foster trust and security.* https://www.intgovforum.org/en/filedepot_download/235/20623

Our distilled findings coalesced around two main themes. They point to a **gap in understanding the roles of a wide variety of actors and stakeholders in mitigating cybersecurity incidents**. And they show a **persistent disclarity in the interplay of norms, policies, and laws**.

2.2. 2022 work plan

The work stream 2 work plan's aim has been to build upon the 2021 report by developing a framework and workflow for similarly collecting and evaluating cybersecurity events, both past and present, with a focus on the storytelling narrative.

The purpose of this workflow is to be prepared to present first-person narratives from those most affected as victims or first responders of cybersecurity events and to connect those first responders and victims directly into the decision making processes about norms at a high level.

Our hope is that in norms development processes the Global IGF's BPF Cybersecurity can present real-world impacts as told directly by most affected voices as a way to ground in reality these high-level policy decisions.

3. Storytelling ….

Storytelling is an effective tool in changing minds, shifting thinking and balancing power. Sharing stories is an exercise in both telling and listening. Recounting an authentic personal experience is not only persuasive, it is an activity that rebalances power relationships between top-down governance structures and everyday lives.

Cybersecurity events make headlines. Often this is because of their sheer scale in terms of which users were affected, dollars lost, or number of consumers affected. However there are always stories to be told in how exactly a case of ransomware, data breach, hardware attack or other event ended up affecting those targeted or incidentally victimised by the incident. There are also those who are alert 24/7 in the event of such attacks that are the first to respond with a code fix, mutual aid or other interventions to victims and affected systems alike. At the end of the day, cybersecurity norms must make a difference in the lived experiences of these people, past, present and future.

Some examples of storytelling in communities that are closely related and relevant to the Internet Governance Forum and UN-level Cybersecurity Norms deliberations include:

- Global Encryption Coalition asks for testimonials from users and providers of encrypted services how encryption keeps us all safe. https://www.globalencryption.org/get-involved/tell-your-story/

4. Developing a Framework for collecting and evaluating cybersecurity events

We ask, "How would specific norms have been effective at mitigating adverse cybersecurity events?"

Last year the Cybersecurity Best Practice Forum of the Internet Governance Forum published a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents.

By writing background briefs for historical cybersecurity events, the authors' review, evaluation and analysis take into consideration the Best Practice Forum on Cybersecurity's prior reports, as well as other published research and reports, aimed to conclude whether and how cyber norms have been successful at mitigating the adverse effects of these events.

In some cases we conclude that important cybersecurity events may have supported norms implementation, or expanded the scope of an existing norm.

In all cases we point to the need to put those most affected by cybersecurity events and first responders in direct contact with policy makers designing norms and laws.

4.1. Collecting details on cybersecurity events with a focus on the voices of those most affected

The following form captures the basic details about cybersecurity events in order to continue to analyse these events against existing and developing norms, with a particular focus on the voices of those most affected by the incidents themselves. The form was developed in an iterative way by the participants in the workstream 2 effort.

Major cybersecurity events

Introduction

Thank you for participating in our survey. The information you share will be used by the IGF BPF Cybersecurity and any personally identifiable information is kept fully confidential.

How would specific norms have been effective at mitigating adverse cybersecurity events? In 2021 The Cybersecurity Best Practice Forum of the Internet Governance Forum published a discussion paper that interrogates which are the core ideas behind prominent cybersecurity normative agreements that had the most continuity through various incidents. By writing background briefs for historical cybersecurity events, the authors' review, evaluation and analysis take into consideration the Best Practice Forum on Cybersecurity's prior reports, as well as other published research and reports, aimed to conclude whether and how cyber norms have been successful at mitigating the adverse effects of these events.

In some cases we conclude that important cybersecurity events may have supported norms implementation, or expanded the scope of an existing norm.

In all cases we point to the need to put those most affected by cybersecurity events and first responders in direct contact with policy makers designing norms and laws.

This form captures the basic details about cybersecurity events in order to continue to analyse these events against existing and developing norms, with a particular focus on the voices of those most affected by the incidents themselves.

Read more about the IGF BPF Cybersecurity's analysis and findings on *'Testing norms concepts against cybersecurity events'* in section 2 of last year's report (p. 50-76) at https://www.intgovforum.org/en/filedepot_download/235/20623 .

More on the IGF BPF Cybersecurity at https://www.intgovforum.org/en/content/bpf-cybersecurity

Questionnaire

1. Name of the Event **(*required)**

2. Date

3. Type of Event

   - ☐ Advanced persistent threat (APT)
   - ☐ Data breach

- ☐ Data leak
- ☐ Denial of Service (DOS) or Distributed Denial of Service (DDOS)
- ☐ Malware
- ☐ Supply chain attack
- ☐ Technique disclosure (eg Snowden Revelations)
- ☐ Vulnerability
- ☐ Control systems breach
- ☐ Dual-use software
- ☐ Disinformation campaign
- ☐ Ransomware
- ☐ Social engineering
- ☐ Other

4. Country/countries (of the attack)

5. Target

6. Intent

7. Description **(*required)**

8. Outcomes/response

9. Elements of response/outcomes

    - ☐ Cybersecurity norms helped with mitigation
    - ☐ Influenced new or existing cybersecurity norms
    - ☐ Security research
    - ☐ Cross-sector cooperation
    - ☐ Cross-border cooperation
    - ☐ Political/legal/technical attribution
    - ☐ Other

10. Three secondary sources for reference (URLs)

11. Your name and contact information for follow-up questions

Consent

- ☐ If you have shared your contact information it will be kept fully confidential.

5. Next Steps

Now that our framework is in place, we hope in 2023 to begin in earnest to populate it with stories that are collected from networks of first responders. We hope that those first responders can also help connect us to the victims of past attacks.

Measures of success of this work in 2023 should be:

- Whether we are able to collect stories of emerging cybersecurity incidents in 2023,
- Whether we can use storytelling directly in the cybersecurity norms deliberations at the UN-high level in 2023.

Acknowledgements

Contributors to the work of the BPF Cybersecurity workstream 2

Mallory Knodel (Workstream 2 lead & Editor), Anastasiya Kazakova, Allison Wylde, Evan Summers, Wim Degezelle (IGF consultant).