Report on the Activities of the IGF Best Practice Forum (BPF) for: Establishing and supporting CERTs for Internet security

Cristine Hoepers, CERT.br/NIC.br

Maarten Van Horenbeeck, FIRST

Adli Wahid, FIRST

Background: Internet Governance

Internet Governance Forum (IGF)

- established by the World Summit on the Information Society in 2006, intended to be the leading global multi stakeholder forum on public policy issues related to Internet Governance.

  http://www.intgovforum.org

NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance

- a one-time event, convened in São Paulo, Brazil, to discuss the future of Internet Governance, ICANN and IGF

  http://netmundial.br/

What are the IGF BPFs

The NETmundial statement called for a strengthened IGF

"Improvements should include inter-alia:

Improved outcomes: Improvements can be implemented including creative ways of providing outcomes/recommendations and the analysis of policy options;"

http://www.netmundial.org/references/

As a result the IGF created 5 BPFs to provide outcome documents related to:

1. **Developing meaningful multistakeholder participation mechanisms**
2. **Regulation and mitigation of unwanted communications (e.g. "spam")**
3. **Establishing and supporting Computer Emergency Response Teams (CERTs) for Internet security**
4. **Creating an enabling environment for the development of local content**
5. **Best practices for online child protection**

http://www.intgovforum.org/cms/igf-2014/best-practice-forums

Background: NETmundial Security Statements

"Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. ***Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders****."*

*"****Initiatives*** *to improve cybersecurity and address digital security threats* ***should involve appropriate collaboration among governments, private sector, civil society, academia and technical community.****"*

*"****There is room for new forums and initiatives. However, they should not duplicate, but add to current structures.*** *All stakeholders should aim* ***to leverage from and improve these already existing cybersecurity organizations.*** *The experience accumulated by several of them demonstrates that,* ***in order to be effective, any cybersecurity initiative depends on cooperation among different stakeholders, and it cannot be achieved via a single organization or structure.****"*

BPF on the establishment of CERT teams for Internet Security

Experts invited to participate in a multi-stakeholder discussion, leading to the development of best practices

- discussion via an open mailing list
- online virtual meetings
- 90 minute session at the IGF 2014

Lead Experts:

- Cristine Hoepers, CERT.br/NIC.br
- Maarten Van Horenbeeck, FIRST
- Adli Wahid, FIRST

UN Consultant:

- Wout De Natris

Online documents, resources and mailing list:

http://www.intgovforum.org/cms/170-igf-2014/best-practice-forums-2014/1893-establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security

Template for the BPF Report

1. Definition of the issue
2. Regional specificities observed
3. Existing policy measures and private sector initiatives, impediments
4. What worked well, identifying common effective practices
5. Unintended consequences of policy interventions, good and bad
6. Unresolved issues where further multistakeholder cooperation is needed
7. Insights gained as a result of the experience
8. Proposed steps for further multistakeholder dialogue

Summary of the BPF Work as Presented at the IGF Main Session

What is a CERT/CSIRT?

"*A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for* ***receiving, reviewing, and responding to computer security incident reports and activity****. Their services are usually performed* ***for a defined constituency*** *that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client.*"

"*An Incident is any* ***real or suspected adverse event in relation to the security of computer systems or computer networks***."

Source: CERT/CC CSIRT FAQ

1) Insights gained (part 1/2)

- **Preference of term ‘CSIRT’ over ‘CERT’**
  - **incident response, as captured in CSIRT, Computer Security Incident Response Team, better captures what CSIRTs do**
  - **‘emergency’ may lead to misunderstandings and misconceptions about the work on hand**
- **There are different types of CSIRTs. Their constituencies and services may differ, but they are connected by their goals of mitigating incidents on behalf of a constituency.**
- **CSIRTs have been working together and sharing information for many years. Much of this is due to that most CSIRTs need to respond to similar threats.**
- **Success of a CSIRT is tied to correctly determining deliverables, and their perception with other stakeholders.**
- **Many best practices exist and are freely shared, resulting out of trusted relationships and existing collaboration.**

2) Insights gained (part 2/2)

- The role of the government is very delicate. Top-down approaches from governments on creating CSIRTs do not always work well. A bottom up approach was preferred over top down development. Everything has to do with Trust.
- Cooperation is rooted in trust. Legislation does not provide trust, it is built up over time, by delivering what is needed.
- There is a need for “CSIRT of last resort” for a country - a team which can take at least some level of ownership if no other parties exist.

3) Unresolved issues

- Further discussion is warranted on the National CSIRT definition, and the definition of a “CSIRT of last resort”
- Need to open the document up to other communities to find better ways of collaboration
- Cost of participation of developing countries in the CSIRT community and its international processes is interesting for future debate. What priorities can be set, and how can this type of work be funded?
- Is there a role for CSIRT teams in addressing the root causes of incidents, such as prevention of cybercrime. This is an area ripe for multi-stakeholder discussion, e.g. with law enforcement

4) Proposed steps for multi-stakeholder dialogue

- We need to find mechanisms to raise challenges the CSIRT community faces to the relevant stakeholder groups. We can do so by inviting other stakeholders to international CSIRT meetings, or share knowledge at stakeholder events.
- Inputs are needed to reflect multi-stakeholder requirements for establishing and ensuring success of CSIRTs

Some Highlights from the IGF Session Discussing the Best Practices Document

CSIRT History and Cooperation

- CERT/CC was the first CSIRT, created in 1988 in response to the Morris worm incident

- CSIRTs form a cooperation network
  - there is no hierarchy
  - the cooperation is based on trust
  - it helps organizations to improve their own security and simultaneously this improves the whole Internet ecosystem security

Existing CSIRT Forums

- APCERT, **Asia Pacific**
- AfricaCERT, **Africa**
- LAC-CSIRTs, **Latin America and Caribbean**
- OIC-CERT, **Organisation of The Islamic Cooperation**
- TF-CSIRT and EGC-CERT, **Europe**
- FIRST, **Global**

Definition of the issue

b.1) What is a CSIRT?

- there are CSIRTs in many and very different organisations that can have
  - different objectives
  - different naming
- there are CSIRTs within **government** organisations, **academia**, **private organisations** and CSIRTs with **a national task**
- there are organizations that only work for its own constituency and organisations that assist their customers or provide CSIRT services to other organisations
- there is a consensus that a CSIRT is **a team of experts** that responds to computer incidents, **coordinates on the resolution**, notifies its constituents and **assist the mitigation** of the incident.
- CSIRTs are involved in **"technical mitigation"** of computer incidents relating to **"internet health and risk reduction"**

Regional Specificities observed

Cyber Security incidents can not be mitigated by a single country or entity, collaboration is required

- This leads to some expectations on common capabilities, process or tools among the CSIRTs.
- While there are information sharing platform the challenges include taking this globally and establishing trust

Inputs from Discussants

- Asia Perspective
- South America Perspective
- European Perspective
- African Perspective

a. Policy Discussion

- ITU, EU, African Union & APECTEL have all called on member countries to establish cyber security strategies and incident response capabilities

- Questions:
  - Is the level of ambition roughly in balance between regions?
  - Are activities noticeable in all regions/continents at the same pace?
  - Do best practices and guidelines reach each region in the same way?
  - Can representatives from regions (financially afford to) participate in the same meetings?

b. Services & Regional collaboration provided by CERTs/CSIRTs

- A number of global, regional and national incident response forums exist and organize activities & information sharing
- Physical meeting is important to get acquainted and establish trust for future cooperation

c. The cost of a CSIRT

- Cost will vary regionally and between organisations depending on constituency and services provided
- Some common cost items include salary, equipment and tools, travelling to conferences or meetings.

d. Legal Systems

- Although legal systems vary from around there world, this has not stopped CSIRTs from collaborating and supporting one another.
- There is consensus that cooperation beyond jurisdiction is to be encouraged in other regions of the world

IGF BPFs Next Steps

The Best Practices Forums will remain active until the 10th IGF Meeting

- **scheduled to take place in João Pessoa, Brazil, on 10-13 November 2015**

The first outcome document will be finalized in October/2014

The discussions will continue based on the first outcome document

http://www.intgovforum.org/cms/igf-2014/best-practice-forums

We are looking for

- **more stakeholders to join the discussion**
- **feedback on the unresolved issues, specially regional specificities**

A new outcome document, as a result of the next year's debate, will be presented at the 10th IGF

Thank You!

Cristine Hoepers, CERT.br/NIC.br
cristine@cert.br

Maarten Van Horenbeeck, FIRST
maarten@first.org

Adli Wahid, FIRST
adli.wahid@gmail.com