IGF 2017 Report

"Critical Issues in Improving Cybersecurity Incident Response"

- *Session Title:*
Critical Issues in Improving Cybersecurity Incident Response

- *Date:* December 18th, 2017

- *Time:* 11:30am – 13:15pm

- *Session Organizer:*
Maarten Van Horenbeeck , FIRST (Technical Community)
Michael Carbone, Access Now (Civil Society)

- *Chair/Moderator:*
Gustaf Bjorksten, Access Now (In-person moderator)
Adli Wahid, FIRST (Remote moderator)

- *Rapporteur/Notetaker:*
Maarten Van Horenbeeck, FIRST

- *List of Speakers and their institutional affiliations*:
Cristine Hoepers, General Manager, CERT.br (Technical Community)
Audrey Plonk, Senior Director, Global Cybersecurity Policy, Intel Corporation (Private Sector)
Grace Githaiga, Co-convenor for the Kenya ICT Action Network (Civil Society)
Mallory Knodel, Association for Progressive Communications (Civil Society)
Pedro Veiga, Deputy Director, NCSC -PT (Government)

- *Key Issues raised (1 sentence per issue):*

- Information overload has in some cases led to an over-reliance on automation, which is degrading trust, as there are often misunderstandings behind the impact of an incident or abuse report.
- The network of cooperation that CSIRTs have built only works effectively when there is trust between organizations. This trust can be affected by where a CSIRT is positioned, and what organizations it is experienced at working with.
- How are Human Rights baked into the work of incident responders?
- Technical expertise is now more commonly criminalized. This makes it more difficult for incident responders to effectively deal with incidents, and for capacity to be built.

- *If there were presentations during the session, please provide a 1-paragraph summary for each presentation:*

There were no presentations during the session. There were opening comments which have been integrated in other parts of this report, as they covered the same topics.

- *Please describe the Discussions that took place during the workshop session (3 paragraphs):*

A main topic of discussion was to share bad and/or good experiences that stakeholder groups have had reporting security incidents to CSIRTs. In this discussion, it was identified that a critical component of sharing involves the need for any organization to have a contact which is responsive, and that the report must be adequately handled. An interesting observation was that as we're spending more effort working on automating processes, we sometimes miss the significance behind "why" someone is reporting a security incident, or abuse. This can sometimes lead to the CSIRT determining an issue is not a security issue, without providing detailed guidance on why it is not, and without an opportunity for the reporter to refute this determination. One way this challenge could be addressed is by ensuring civil society, and other stakeholder

groups that sometimes may feel misunderstood, to participate in technical community and CSIRT events, and share their experiences. There may also be value in more regional and local cooperation and events that help build communities of knowledge, where specific problems are likely to be most understood. Finally, there is a need for more people to become well trained on incident response – and a real value in growing the community of sectoral CSIRT, which typically have a similar understanding of the basic problems their constituencies face.

The panellists also discussed how raising incidents to the right stakeholders quickly can be challenging, but is a core function of a CSIRT. The example was raised of financial institutions, which originally were concerned about sharing information, but quickly realized that an incident which undermines trust has the ability to affect the entire sector. They became strong supporters of the concept.

There are configurations in which raising issues, and cooperating across organizational boundaries, become troublesome. A core concern is where a CSIRT is located. For instance, a national CSIRT that focuses on protecting national infrastructure may be limited in dealing with incidents that do not directly affect that infrastructure, but have impact beyond national security. In addition, a CSIRT positioned in an intelligence agency may not be widely trusted, or may have classification challenges in sharing information with others. Quite often, it is good to have CSIRTs with very specific responsibility, but have a "CSIRT of last resort" that works with the entire community and takes the main coordination action. There is no one-size-fits-all, though, and these challenges must be considered when CSIRTs are developed and expected to work successfully with others.

The group discussed how human rights are baked into the work of CSIRT. In an example stated during the session, support for human rights came from the top, with the organization developing principles aligned with the UN Declaration of Human Rights, and then translating these to tactical decisions through the development of policies and individual discussion with technical stakeholders. This was particularly important in engaging with external stakeholders. It was noted this may affect cooperation with other third party organizations, such as CSIRT in governments, where there may be concern arounds human rights implementation.

An issue raised was the criminalization of technical expertise. This covered areas such as arrests of security trainers, encryption and the use of VPNs. A panellist noted that today we are seeing several "knee-jerk responses" rather than measured responses based on an assessment of the actual security situation. This can lead to interference with innovation. Asked how CSIRTs can push back, it was noted that in debates such as "exceptional access" and encryption, it is very important for the technical community and private sector, to educate government on the technical challenges and trade-offs involved. Many concepts from the pre-Internet era are being pushed to law enforcement online, without understanding that the trade-offs in the Internet realm can be quite different.

Two questions from the audience deserve special note due to the lengthy discussion:

- A questioner asked how CSIRT can help develop good practices. Today, CSIRTs share information around incidents, but do not always make it available externally to the wider community. As a result, organizations may be compromised through the same mechanisms as previous compromises. Repeated compromise can drive business away from small and medium enterprises, or from countries with more limited cyber security capacity. Another questioner asked a similar question, how it is possible that CSIRT have "information overload", as was discussed in the session, whereas little information is available to small and medium enterprises. *It was noted that organizations often have limited cyber security expertise to interpret some of the more detailed sharing that takes place in the CSIRT community. That information is typically summarized and shared by CSIRT to their communities, but not in all cases. One panellist noted how CSIRT often share recommended actions, based on their analysis of these incidents, rather than deep technical detail on individual compromises, and that these actions of "basic hygiene" are critically important to preventing compromise. It was also by another panellist that smaller organizations should be recommended to invest in cybersecurity capable IT resources to have at least some capability to be able to leverage the information made available to improve their defences.*

- A questioner challenged the panel by asking if the CSIRT community, and its model of cooperating between "pockets of trust" that have built within communities, can continue to scale. A panellist noted the work of the IGF Best Practices Forum on CSIRT on identifying reasons how trust develops, and that if widely considered, trust in this way can continue to develop. Another panellist noted how there is value in transnational, non-state bound CSIRT that help promote sharing between wider communities, rather than on the local level, and can help bring new "local" CSIRT into that wider community. Finally, it was raised that such CSIRT, as well as topic/community-focused organizations often have funding constraints, and that this is something which needs to be addressed for the community to continue to develop.

- Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

- A participant from the technical community raised that it is critical for government, the incident response community, civil society and private sector to come around the table and educate each other on their respective concerns regarding encryption. There is too little technical debate on the challenges and risks involved, and little actual ongoing debate. Technical community members should actively educate and create awareness around the technical challenges of certain proposed solutions on cybersecurity.
- A civil society participant raised that there should be more "civil society aware" CSIRT, who understand the challenges this stakeholder group faces. It's difficult and expensive to build all technical expertise in the civil society community, so creating CSIRTs specifically to support them is more challenging than educating CSIRTs on how they can cooperate with civil society. Suggestions that were raised included having more civil society participation in CSIRT conferences.
- The role and configuration of CSIRT is to be carefully considered when a new CSIRT is being built. For instance, when a CSIRT is part of a national intelligence capability, sharing with that CSIRT may be more difficult for various stakeholders. In addition, greater secrecy within that CSIRT may limit its ability to cooperate. Previous work in the IGF Best Practices Forums on Cybersecurity and CSIRT also indicated this limitation. Having sector or organization-specific CSIRT is a must, but a "CSIRT of last resort" may be able to provide additional methods of communication between those organizations and others, under rules that are better understood by all stakeholders.
- A question that was raised by audience members, and which may be worth further consideration, is how information can be made to more effectively flow to small and medium enterprises. It was noted that these organizations often do not invest in the basic cyber security capability to process the information currently available.

The outcome from this session, including video recording, transcript, and this summary, will be contributed to the FIRST Special Interest Groups on Ethics, and the IGF Best Practices Forum on Cybersecurity, for further consideration and discussion.

Gender Reporting

- Estimate the overall number of the participants present at the session:

There were approximately 60 total participants

- Estimate the overall number of women present at the session:

Approximately 20 participants were women. The panel itself was gender balanced, with three out of five speakers being women.

- To what extent did the session discuss gender equality and/or women's empowerment?
- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:

The session did not directly address issues related to gender equality and/or women's empowerment. However, it did consider challenges in how technical community, government and public sector security teams can successfully cooperate with civil society organizations.