Internet Governance Forum (IGF) 2014

Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security

Executive Summary

Major findings

Originally, the Multistakeholder Advisory Group (MAG) had agreed for this Best Practice Forum (BPF) to deal with Computer Emergency Response Teams (CERT). However, in the preparatory process for the Istanbul meeting it emerged that the experts involved found that the acronym CERT was ill chosen, if not confusing, and this for various reasons. Among the reasons cited was the fact that the acronym CERT is a registered trademark of a US university, and therefore cannot be freely used. Maybe more importantly, however, was the substance of the work involved. The daily routine of the work relates to "incidents" rather than "emergencies", and the experts felt that a focus on the latter could be detrimental to the trust in the global cooperation among the security teams.

The experts unanimously agreed to change the term in the title of the BPF to Computer Security Incident Response Teams (CSIRT) instead, as this would reflect better the very nature of their work. They also felt that it was important to understand that CSIRT come in many shapes and sizes, which are not hierarchically organised. Each CSIRT is autonomous, serving its own constituency according to described goals and agreed upon services. A CSIRT can operate within a government, an organisation, a company, serve one product and even be a commercial offer. While coordination and cooperation at the national level was seen to be important, the point was made that this should be a voluntary choice, based on trust.

The model of national CSIRT was discussed at some length. The main conclusion that emerged was that the only chance of success is when other CSIRT accept and trust each other and engage in voluntary cooperation. Any top-down enforcement of cooperation was seen as potentially counter-productive, as it could have a negative effect on the will to collaborate with each other, both at the national and international level. Therefore, one of the major conclusions of this BPF was that it would be helpful to engage in and intensify the dialogue with governments.

Another conclusion was that CSIRT have organised themselves well. There is a common understanding of what a CSIRT should be, involving successful communication, cooperation, training, development and dissemination of good practices.

CSIRT's work is sensitive for many reasons. For example, it involves vulnerabilities, reputations or privacy sensitive data that have to be exchanged to mitigate cyber incidents or threats; this requires work on building high levels of trust between organizations and individuals. Trust is the basis of cooperation. Trust is built during meetings, through trustworthy responses to cooperation requests, through working, training and developing ideas and solutions together. Trust is key, something all stakeholders need to understand.

There was a rough consensus that there is no need for new descriptions or global standards. There are enough examples and "good practices" to choose from when starting a CSIRT.
One of the conclusions is that not all countries can benefit from the existing global and regional structures, due to a lack of resources (or the total absence of a CSIRT). Capacity building is needed here, as well as an understanding that travel costs have to be included in the budget of a new CSIRT. Knowledge and trust grow fastest this way.

There is a strongly felt need to engage with other stakeholders. First, in order to take away misunderstandings about the way CSIRT work, are functionally placed and organised. This misunderstanding can lead to other stakeholders making ill-advised decisions, that ultimately lead to a break in trust and thus an end to previously successful cooperation between CSIRT (in other countries). And, second, in order to explore (and perhaps define ways towards) enhanced cooperation in the future.

Suggestions for future work

Many suggestions were made to improve the cooperation framework between existing CSIRT, future CSIRT and other (regulatory and enforcement) agencies, including through the establishment of a national point of contact. In what way can CSIRT assist each other in cooperation or capacity building and in what ways can CSIRT in the future, perhaps, cooperate differently (with third parties) on a voluntary basis? These questions need further debate among all stakeholders, including those who did not engage in this BPF.

The following eight issue areas were seen as lending themselves for further multistakeholder debate, where progress can be made. Other issues need further clarifications and discussions among CSIRT first and are not included here.

a. Misconceptions regarding the functions and tasks of CSIRT. Misconceptions lead to misunderstandings that can seriously influence the performance of a CSIRT and thus the performance of fellow CSIRT. Cooperation and the development of CSIRT in different parts of government is an area that needs further development and discussion.

b. The mitigation of incidents involves sharing (privacy sensitive) data. There is a clearly identified need to discuss this topic further with governments and (privacy) regulatory agencies.

c. National Point of Contact or CSIRT of last resort. The call to have such a point in as many countries as possible is evident. There is a need for further discussion on its functions and how to achieve this.

d. Privacy and free speech. There are concerns in how far (the work of) CSIRT impede on free speech, as well as in what way CSIRT can contribute to a higher privacy standard in the world.

e. The implementation of good standards. There is a need for swifter implementation of Internet standards and good practices in general and at CSIRT level in particular.

f. Cooperation with law enforcement (LEA) and other regulatory agencies. Mandatory cooperation with LEAs tends to lead to a lesser trust between CSIRT. On the other hand, there is a possibility to cooperate more on a voluntary basis. This thin line is worth discussing further with other stakeholders involved.

g. Schooling, education and participation in international meetings. The importance of this topics cannot be underscored enough if a successful CSIRT is a nation's goal. Capacity building and CSIRT is a topic that needs to be brought further.

h. The development of case studies. There is a need for extensive case studies, such as those on DNSChanger and Conficker, in the light of (the implementation of) lessons learned, potential cooperation with other stakeholders and reporting mechanisms in different jurisdictions.

Report

In the past months, this Best Practice Forum has discussed the issue of establishing and supporting Computer Emergency Response Teams from different angles. This paper is the outcome document of this discussions that were held up to October 2014. The debate that unfolded between the participants ranged wide and touched upon fundamental issues in many and very different ways. This outcome document cannot be seen in any way as a final document. There are many questions left to answer, topics to address and absent stakeholders to involve. It is best seen as a starting point for further debate and discussions in 2015, working towards the Internet Governance Forum in 2015 in Brazil.

1. Definition of the issue

a. Introduction

In the past months, experts from around the globe have discussed and delivered input to the forum on CSIRT (Computer Security Incident Response Teams). This fruitful collaboration has brought forward in-depth insights into the work done by the different CSIRT and the good practices published by different organizations that document this. Also, some misconceptions that non-CSIRT stakeholders sometimes have were brought to light, as were substantial regional differences, both of which at times hinder successful cooperation and incident mitigation. An important factor that was brought up is that the work of CSIRT is frequently sensitive, as CSIRT have a need to share and exchange information with other CSIRT and even victims. In order to be successful, a CSIRT must be sensitive to the need to protect shared information and to develop and maintain trust.

This document tries to capture the accomplishments as well as the challenges facing CSIRT. Some of these have to be taken up within the community, while others may only be solved by engaging more with other stakeholders, as will be shown below. This document follows the template provided by the Multistakeholder Advisory Group of the Internet Governance Forum and is structured accordingly.

b. Topics that define the issue

The following paragraphs define the topics that came up during the online discussions, that were quite extensive and covered several very different issues.

i. What is a CSIRT?

CSIRT exist in a variety of different organizations, both in the public and private sector, with a variety of different mandates, authorities and even names. There are organizations which only work for their own constituency or its own product security (a PSIRT) and organizations that assist their customers (as well) or hire themselves out as a CSIRT to other organizations. Finally, there are CSIRT with a national task in ensuring coordination between all stakeholders involved in an incident and/or are there to protect vital/critical infrastructure.

Despite all the differences that can be pointed concerning the originating background of varioust CSIRT, there is a consensus that a CSIRT is a team of experts that responds to computer incidents,

coordinates their resolution, notifies its constituents, exchanges information with others and assists constituents with the mitigation of the incident. The forum prefers to see CSIRT as a technical actor. CSIRT are involved in "technical mitigation" of computer incidents relating to "Internet health and risk reduction". The forum acknowledges that additional tasks for a CSIRT can include preventive measures and educational reach out within its constituencies to proactively prevent incidents from happening. In the recent past, CSIRT have evolved increasingly towards becoming a bridge between various communities of trust. This has required the CSIRT to be fluent in the language of business, technology and diplomacy.

ii. CERT or CSIRT?

The forum preferred other terms over the name CERT, Computer Emergency Response Team[1], as the word takes away from the work that is more standard procedure for the teams working in this field: incident response, as captured in the term CSIRT, Computer Security Incident Response Team. The choice of wording for 'emergency' leads to misunderstandings and misconceptions about the work on hand. This is especially the case for those not directly involved in the work. The topic is discussed more in-depth below, in the section on impediments. The European agency ENISA underscores this part of the debate: "At the moment both terms (CERT and CSIRT) are used synonymously, with CSIRT being the more precise term[2]". The traditional used name, writes ENISA, is CERT, but the current work, including e.g. alerts, trainings, security advices, etc., undertaken by CSIRT makes the name CSIRT more accurate. This forum will exclusively use the latter name here and changed the BPF title accordingly.

iii. CSIRT of last resort

A topic that was broadly discussed was a CSIRT of last resort. Ideally, the CSIRT of last resort is a national point of contact (POC) within a country, that allows for and coordinates cooperation within that country with the organizations that are either involved in, causing or affected by an incident. It is the CSIRT someone can turn to, when there are no other known contacts within a country. Any other variety, regional or global, is also welcomed, should it be effective. Below we will get back to this topic.

iv. National CSIRT

The previous point overlapped somewhat with the discussion about a national CSIRT. There is no consensus on which institution ought to be the national CSIRT. Several people presume that this always should be a government institution or agency, but this is contested by others in the forum, who showed different examples. Over the past years, more and more national CSIRT have sprung up, sometimes more than one per country. In these situations, there may be a commercial or volunteer CSIRT that has provided services for some amount of time, which is then joined by a new governmental or commercial CSIRT offering similar services. Crucial to this development is that new CSIRT take care to establish trust and good relationships with the existing CSIRT, and there is clarity in role and responsibilities. Given the coordinating role of the CSIRT, cooperation between CSIRT is crucial, even when their constituency partially or completely overlaps. The community, i.e. those who have been cooperating over many years, broadly saw potential issues in this space and flagged it as an area of concern, where a new CSIRT must tread carefully.

[1] The term "CERT" is actually a registered trademark of the Carnegie Mellon University. In order to carry the name officially, it has to be licensed from CMU.
[2] https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

Discussion in the forum showed that there are many different CSIRT models used across the world, which all appear to have their own benefits and disadvantages; such differences can be related to who hosts a national CSIRT, or what services it should provide, as well as to other issues like funding, local Internet governance structure and cultural issues, among other factors that might impact the decision of creating a CSIRT. From experience, each country will need to identify what works best in its case. Examples that were provided show that there are many different sorts of (national) CSIRT, with very different backgrounds, ranging from 100% government run, independent agencies to an organization run by volunteers[3]. It was also mentioned that, in some countries, CSIRT are integrated in ccTLDs (country code top level domains) registries or work closely together with them. From the debate in the forum it can be derived that most agree that "the most important of all is that these CSIRT work in cooperation to make the Internet more stable and secure".

Some concern was expressed around the term "national CERT/CSIRT", and the fact that it is not clearly defined. This term is used for different types of CSIRT, which focus on different constituencies and provide different services. There is opportunity here for the community to develop a better definition. Using the term "national" for a CSIRT does not necessarily mean it is a national CSIRT in tasks, constituents and deliverables, nor that it functions as one, nor that it is perceived as one by its colleague CSIRT. It is important for governments and other stakeholders to understand that security is not dealt with in one organization, but in each individual organization separately. Another topic of concern was how to ensure that information provided to another CSIRT or organization is used appropriately. This is a very important question for CSIRT.

One comment introduced a completely different angle to the national CSIRT discussion: privacy and free speech. It poses that a government or national CSIRT should have a mandatory clause in their statement that ensures transparency and guarantees them a practical veto in case politically motivated requests or incidents appear. This is a topic ripe for further discussion, as any government institution will be expected to implement adherence to law.

There was consensus in the forum that a CSIRT calling itself a "national CSIRT" must define publicly what its constituency is and what services it offers, and thus take away any misunderstandings at the very beginning. This is not such a different requirement from all other CSIRT, but it is more important for a "national CSIRT".

There are two strong diverging opinions on how an organization can become a national CSIRT. The first is that a government can institute a national CERT and domestically require or request all constituents to report incidents to it, forcing or otherwise motivating cooperation. If an organization has not garnered the necessary trust, which is often the case for an entirely new CSIRT with no history of working with peers, this may lead to it not being able to partner with other international organizations which may not be formally required to report to it. The second opinion states that a national CSIRT has to take account of teams and activities that have already been created from the bottom up. This document discusses this topic extensively below.

It was suggested to draft a template for the type of communications one might encounter when dealing with a (new) "national CSIRT". The answers will help to establish what a national CSIRT is, what is does and who its constituency is. RFC 2350 ("Expectation for Computer Security Incident Response")[4] was an early attempt to develop a way for a CSIRT to specify its services and constituency, but it could benefit from more widespread adoption. This will benefit other

[3] A full list can be found here: http://cert.org/incident-management/national-csirts/national-csirts.cfm
[4] https://www.ietf.org/rfc/rfc2350.txt

stakeholders involved as well. The development of good case studies could be an important area for multistakeholder discussion. A number of such case studies already exists, such as the technical community's handling of the DNSChanger and Conficker cases, but there is room for more extensive case study development. One participant noted that it does not appear that many of the recommendations or lessons learned are consistently applied. The field of practice is still evolving very quickly, so case studies may also have a fairly short shelf life of usefulness.

The forum also reached consensus that the discussion concerning national CSIRT is ripe for additional discussion from a multistakeholder perspective.

v. Services of a CSIRT

The services a CSIRT delivers are directly dependent on its constituency and the tasks given to it. Having said that, three main service categories can be identified:

1. **Reactive services**. These services are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.
2. **Prevention services**. These services provide assistance and information to help prepare, protect and secure constituent systems in anticipation of attacks, problems or events. Performance of these services will directly reduce the number of incidents in the future.
3. **Security quality management services**. These services augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, audit or training departments. If a CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats and system weaknesses. These services are generally preventive, but contribute indirectly to reducing the number of incidents.[5]

Within each of these services, incident information may need to be shared or stored, and it is crucial that each CSIRT puts in place processes, procedures and techniques to ensure this type of sharing and storage can happen in a secure way.

Connecting services to the constituency means that there are many different models in use across the world. For instance, one CSIRT can only be responsible for the security of one product, where others are responsible for the complete security of large constituencies in both pro-active and reactive ways, including awareness and education.

Another aspect is the trust level CSIRT can establish and maintain within its constituency and its colleague CSIRT, nationally and internationally, which will determine whether the services of a CISRT are used and/or accepted.

A distinction was made in the forum on the services a CSIRT provides to its own constituents and the services it provides to its networks of fellow CSIRT, i.e. (inter)national cooperation between CSIRT. As incidents can be caused by very different actors spread over multiple jurisdictions, on the one hand a CSIRT has to be able to notify colleagues abroad and be able to receive and act upon alerts. These services need to be among the tasks of a CSIRT, in order for it to be effective and

[5] This summary of CSIRT service categories by CERT/CC is followed by an extensive list of services as published by CERT/CC, part of Carnegie Mellon University. See: http://www.cert.org/incident-management/services.cfm

trustworthy. CSIRT which focus on one particular, smaller constituency, such as an enterprise CSIRT at a smaller company, may in some cases elect not to take on this role independently, and may need to use its network of coordination centers or national CSIRT, which are more likely to have an international contact roster or network, to take on this function. As was noted, a CSIRT that does not respond to a request for assistance from its peers will quickly become isolated. There is a strong interdependency in order to be effective.

In the past, several organizations have published documents describing which services a (national) CSIRT has to offer at a minimum. This forum however has reached consensus to call them "good practice" documents, as there is no "best" practice, nor is there a need of one. Practice shows that there are several different ways to be(come) a successful CSIRT. A participant noted that the field of practice is relatively young, and common measures for success are yet to be defined. As part of this effort, several good practice documents were collected and are linked from the Internet Governance Forum website designated especially for these documents[6].

vi. Tooling of a CSIRT

The forum has a consensus view on the fact that the services offered by a CSIRT determine the tools it needs in order to be effective. It is impossible to come up with one standard list. There are some good practices that can help a CSIRT that is setting itself up. The forum also agrees on the fact that a CSIRT without any tools cannot cooperate effectively with its constituency nor with its peers. It was stated that some tools ought to be non-debatable if a CSIRT wants to be successful. While the tool chosen is less important, the ability to perform certain tasks is very much tied to the type of tool being available. For instance, it is difficult to build an incident response process without involving some form of ticketing or workflow system.

The forum encourages teams to seek out tools that already have been developed in the community and have proven themselves. This way, duplication of work is avoided and workload and communications become more standardized. Existing lists of tools are available from organizations such as ENISA[7].

A second set of resources include data feeds. These feeds provide information on malware infections of other incidents across the CSIRT's constituency. While some feeds are only available on the commercial market, many are available at no cost. This type of data can be collected through a number of means, for instance through the analysis of malicious code samples, monitoring of active attacks on a network, or the sinkholing of malicious domains. Due to the complexity of the problem space and the distribution of information on attacks, a single organization rarely has access to all information relevant to a particular CSIRT's constituency. ENISA[8] and CERT Polska[9] provide a good overview of available feeds of information.

vii. Industry cooperation

Two forum members provided an example in which competitors within one sector cooperate. Both sectors identified in these examples - the financial and telecoms sector - had very similar cyber security challenges and decided to jointly operate a CSIRT. The forum sees this development as positive, but provides some serious thoughts to this option in combination with a comment on

[6] http://www.intgovforum.org/cms/best-practice-forums
[7] See the Clearinghouse for Incident Handling Tools, https://www.enisa.europa.eu/activities/cert/support/chiht
[8] E.g. http://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
[9] http://www.cert.pl/projekty/langswitch_lang/en

Information Sharing and Analysis Center (hereafter: ISACs). This example is very different from the ISAC model used by (critical infrastructure) sectors in other countries and even regions. In this model a member operates its own CSIRT, but meets with his fellow ISAC members and shares information and lessons learned around incidents and threats with them.

The forum discussed that the former model of jointly operating a CSIRT could be a good way forward for countries and companies that are at a relatively low level of maturity and are (in the process of) setting up a new CSIRT. For countries and companies that have more mature CSIRT, the ISAC model could be more effective. The forum gave a general warning that if a company decides to hand over its CSIRT capabilities to a collective CSIRT, it essentially loses control over how incidents are reported to it, but it also loses some of its ability to respond. It becomes more dependent on the collective CSIRT. The forum added that an ISAC model does not have this impediment. Various information sharing and coordination models exist, and some of the considerations involved in considering them are specified in existing good practices documents, including those by the National Institute for Standards and Technology (NIST)[16].

In many cases, private sector organizations may operate their own CSIRT teams. These can either be focused on the network of the organization or on the security of its products. In the latter case, the CSIRT is often referred to as PSIRT (Product Security Incident Response Team). It was pointed out that private sector CSIRT play an important role in (inter)national cooperation, knowledge sharing and capacity building, for instance through their participation in organizations such as FIRST (the Forum of Incident Response and Security Teams)[10]. Private sector PSIRT or CSIRT teams can provide detailed skills and capability in a more narrow topic, as it generally controls more of its network than a national CSIRT which has to respond to incidents across a far more heterogeneous network. In some developing countries, private sector CSIRT are all a country has or they are far in front in knowledge and activity. As the nature of the Internet changes, and government bodies take an increased interest in a secure Internet environment, these organizations can be well placed for government or national CSIRT to partner with.

viii. Management strategies of CSIRT

A discussion was started on whether there are good practices/uniform standard procedures identifiable for managing incidents and the (re-)occurrence of incidents.

There are several manuals or guidelines available that can be freely shared, such as the ENISA "Good Practice Guide for Incident Management[11]". There are also many references to courses and publications of CERT/CC of the Carnegie Mellon University[12] and other institutions. The guide page[13] of FIRST shows many examples of advice. There are also starting manuals available from JPCERT/CC and APCERT.org. The Internet Engineering Task Force (IETF) has published RFC2350: Expectations for Computer Security Incident Response[14]. Others point to NIST 800-61rev2[15], a document of the U.S.'s NIST.

The forum agrees that there is little need for additional development of guidelines outside of these existing efforts. However, one participant flagged that many standards currently focus on the

---

[10] http://www.first.org/ or http://www.first.org/resources/guides
[11] https://www.enisa.europa.eu/activities/cert/support/incident-management which is available in 26 languages.
[12] http://www.cert.org/incident-management/
[13] http://www.first.org/library
[14] http://www.ietf.org/rfc/rfc2350.txt
[15] http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

development of technical capability, and that there is a lack of a clear, normative model for how CSIRT can partner with existing or new partners. This may be an area for future development.

2. Regional specificities observed (e.g. Internet industry development)

With the growth of bandwidth and Internet connections in the developing world, cybersecurity issues that are common to developed nations for at least one decade reach the developing world more and more. There are examples of cybersecurity incidents that could not be mitigated within a single country. This means that methods and tools of mitigation, which have become standard practice for the front runners, have to become common practice around the world. At the same time, cyber threats are becoming more numerous, diverse and sophisticated each day and where the front runners are adapting to a new challenge, for many new CSIRT it is just another part of a deluge. The good side is that there is experience and knowledge to share. The challenge is how to bring this to the world and to build and keep trust between different organizations and countries from around the globe.

a. Policy discussion

The forum noted that in most regions around the world policies were published aimed at countries that are creating a CSIRT[16]. The African Union, the European Union, the International Telecommunication Union (ITU), the Telecommunication Group of the Asian Pacific Economic Cooperation (APEC-TEL) have all called upon its members to take action on this. It is possible to say that in most countries the topic at a minimum has been heard of and probably is on agendas to take action upon. Also, many national strategies call for a national CSIRT to be in place to deal with incidents as a coordinating team and to assist in dealing with incidents. Facilitating communication, establishing or participating in trust networks and communicating externally are some of the key roles expected from such an organization in a crisis situation or major incident.

Important questions for the community to address are:

- 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?

Working in cybersecurity calls for certain levels of education and experience. Discussion in the forum showed that there are clear differences in knowledge and access to knowledge. In addition, it was flagged that there are not always good standards and credentials to determine and assess experience. This is particularly the case for the CSIRT community, where only part of the work is technical. The other part is working effectively as a team.

b. Services & Regional CSIRT /collaboration provided by CSIRT

Several of the above questions are answered by the way the CSIRT community has set itself up regionally around the globe. A number of regional and global incident response forums exist and they regularly organize both technical and high level meetings.

[16] The group will present a list on regional initiatives online. Any additions are welcome.

Attending meetings is of great benefit for CSIRT employees to get acquainted, establish a first level of trust in order to cooperate together and share data. It is a great learning experience as well. For developing countries, it is not always possible to find funding to travel across the world, let alone organize a meeting itself. However, the need is there. From all sides. Knowledge exchange is necessary. This may change due to the acuteness of challenges that governments and organizations face. More serious incidents can lead to more direct action and priority setting. It remains a focus point for this forum for further discussion in a multistakeholder environment.

c. The cost of a CSIRT

The costs of setting up a CSIRT will vary regionally. There will be costs that are marginally the same, e.g. when devices, tools and software need to be bought from international vendors. However, import costs and taxes may make these tools less easy to acquire in particular regions. The highest cost within a CSIRT usually consists of employee wages. These will strongly vary regionally. They also depend on the number of people working within an organization and ultimately on the size of the CSIRT, the size of the constituency, and the services the CSIRT wants to offer. Also, there can be import restrictions, e.g. an embargo on certain crypto features that may have influence. Finally, there is no general standard which helps a new CSIRT understand how it should size in individuals in relationship to the size of the networks or constituencies it protects.

Valuable advice has come from the forum on what to include in the budget of a new CSIRT. This includes costs for training the staff, as well as travel costs, as conferences are very important to attend for the reasons outlined above.

d. Legal systems

Legal systems vary around the globe. This is a given for CSIRT. One example that was mentioned is the work done by ENISA (European Network Information Security Agency) on behalf of national CSIRT (to be) in the European Union. In view of the differences among political systems and jurisdictions in the world, the outcome of the processes of ENISA constitute only one example of a possible way forward, which may, however, not be easily exported to other countries or regions. However, a partnership between bodies such as ENISA and the technical community can be fruitful.

There are other examples of regional cooperation, e.g. in Asia. Here, cooperation is actively promoted, even regional teams are being set up and collaboration goes beyond national borders. Even though jurisdictions are very different, several organizations across Asia, like the Asian Pacific CERT (hereafter: APCERT), APEC TEL and the Association of Southeast Asian Nations (hereafter: ASEAN) are promoting international cooperation between CSIRT and facilitate the processes of education, exchange of good practices and assist in the first level of building trust: bringing people together to share experiences. The forum agrees that these are examples of cooperation beyond jurisdictions that are to be encouraged in other regions of the world.

3. Existing policy measures and private sector initiatives

a. Policy discussion

History shows that CSIRT have come into place in many countries over time, simply because there was a need for them somewhere in the past 25 years. This could have happened in response to a specific incident, a series of incidents or through other forms of awareness creation. In the recent

past, as written under section 2 of this document, there are formal calls from intergovernmental organizations or national strategies to create national CSIRT. On one hand, this can be seen as positive, as there is a call for action and cybersecurity is high on agendas. On the other hand, experience seems to show that a top down approach does not always work. In fact, the forum noted this could often be counterproductive.

There was a strong belief within the forum that without trust and without delivering the services which are expected[17] to be delivered, any CSIRT - but definitely a national CSIRT- is without meaning. Few parties would work with it under those conditions.

The discussion also revealed that because trust is so important for the success of a CSIRT, the role of a government is extremely delicate. At the same time, there can be strong regional differences with regards to what trust means, due to, for instance, culture or jurisdiction. Those who participated in this part of the discussion reached consensus on the fact that, in general, a CSIRT works best when it is built from the bottom up, or rather from within the community, compared to a top down approach, where the CSIRT is deployed and other parties are "required" to partner with it and trust it. Although this is not a universal standard, a community driven approach is recommended.

In the end it all depends on the level of trust that is built through years of working together and living up to promises. Trust is not easily described in legislative wording, nor is it well settled by a mandate from the top. It can be facilitated by tasks, skills, tools and features in the law that allow cooperation and data sharing, but in the end it comes down to the willingness of individual people.

The forum provided examples on positive roles of government in the process. Sharing cybersecurity incident (data) in ISACs is a positive thing. However, it is important and a prerequisite for success that governments indicate that this form of cooperation is acceptable and helpful. There are a number of examples of good implementations of this principle, for instance where government agencies are involved in the operations of the ISACs as well. One particularly important role which was identified for government is their ability to remove barriers for information sharing, as opposed to enforcing compelled sharing. This is an important need which can only be addressed at the policy making level and needs further debate.

There is a tendency in the group that when government or the "national CSIRT" assumes the role to help others involved in incidents, they have a higher level of success. Where things are compelled or mandatory, this chance of success goes down, often due to a reduced sense of trust.

b. Guides to setting up CSIRT

The forum effort has shown that there are many (attempts at providing) manuals and guidelines from around the globe on the creation of CSIRT. The forum debated the question whether there is a need for the current documents to become current good practice for the world. This was answered with "no" - it is acceptable to have a diversified set of guidelines, focused on addressing regional or industry specific concerns. However, there may be opportunities to derive some common goals and steps towards success from the number of guides currently available, and spread those more widely.

[17] Some have warned that expected services may actually vary significantly from the offered or officially instituted services. Potentially adding to less cooperation, misunderstanding and a lack of trust.

c. Legal/law aspects preventing CSIRT from doing their work

The work of CSIRT is delicate and involves working with (privacy) sensitive data. Often a cyber incident cannot be mitigated without handling and sharing this data with other CSIRT and/or a CSIRT's own constituents in order to protect ICT systems and the individual persons involved in the incident and who are behind the ICT systems. Governments drafting legislation, whether on CSIRTs or on privacy, need to acknowledge these delicacies involved in the execution of the tasks of a CSIRT. CSIRT teams should maintain a good working relationship with privacy regulators, as they both contribute to similar goals.

It has been brought forward that cooperation is sometimes impeded upon by legislation. National laws on privacy and data exchange prevent CSIRT from formally sharing data with colleague CSIRT, industry, national anti-botnet centres, law enforcement and regulatory agencies. Although this may be the case, for necessary future cooperation it is important to find out the difference between perceptions and legal reality. It is suggested in the forum that by opening up to other stakeholders involved, the possibility of cooperation can actually be tested and perceptions changed.

The solution may not be new or adapted laws, but a better engagement between CSIRT, governments and (privacy) regulators. The issue of sharing privacy relevant information, and under which safeguards or controls this is acceptable or not, should be addressed in a partnership between these three types of organizations.

A way forward is to directly engage with these stakeholders. The forum sees opportunities for future multistakeholder engagement on this topic[18].

d. Surveillance and net neutrality

Some forum members brought up that surveillance is an impediment to trust and makes cooperation with other countries and other organizations involved in national cyber security harder. When there is a concern of a CSIRT being involved in direct law enforcement or surveillance operations, trust generally tends to be lower than when the CSIRT operates based on information received directly from affected parties.

A concern was put to the forum that net neutrality is breached when, in the light of surveillance, Deep Packet Inspection (DPI) is used in order to be able to work in cybersecurity. In response, it was mentioned that many CSIRT operate without any need for Deep Packet Inspection or awareness of the contents of packets. In some cases, having this ability may contribute, in particular for a CSIRT with a narrow, single-organization constituency, to mitigating an incident.

A question was presented on how the good can be separated from the bad. In answering it, it was mentioned that, with encryption on the rise, the use of DPI tends to be limited to same-organization CSIRT, such as enterprises, where cryptographic keys are centrally controlled. Most CSIRT providing services to multiple organizations ought not to become overly depended on it. CSIRT that provide monitoring services should ensure to follow applicable law and adhere to privacy expectations.

[18] The need to be able to share (privacy sensitive) data also has come forward when (inter)national and cross sector cooperation in the fight against botnets and the mitigation of infected devices was discussed in the BPF on "unsolicited communications".

4. What worked well, identifying common effective practices

The way people from the CSIRT community from around the globe cooperate within this forum demonstrates that they are used to exchange information, learn and work together.

The topics that circulated within the forum touch upon a broad array of questions and challenges. They shows that the way CSIRT are used to communicate, cooperate and share knowledge and data works really well. All it takes is the effort to engage. There certainly are reasons for this. For instance, all CSIRT in the end face the same incidents and threats, while there is no need to make formal decisions (on good practices) at meetings. Still, there are examples that others could follow if they so wish. The positive form of cooperation in the forum led to the fact that "good practices" were easily identified and agreed upon. The community has been working this way for years. This as such is a good practice other stakeholders can take notice of. This document presents a number of such examples on successful global, regional and national cooperation.

But while the community has made significant progress, there is more to be done.

Around the world there is a need for education and training on the topic of CSIRT skills. The CSIRT community is known for training each other regularly, for instance at meetings of regional or global forums. An important premise rules here: if your peers are having more difficulty with Internet security than you are, try to use your knowledge to help them to improve. The improvements they implement will also help you be more aware when they detect something is amiss. This works well, but may not be attainable all around the globe. Capacity building is an important driver to help ensure the global aspect of cybersecurity.

There are also some opportunities to better align standards and methods. There are a number of technical and process implementations which are recognized as preferred, and further standardization can help new CSIRT understand which of these are available, and which are likely to allow them to work smoothly with other more established CSIRT.

Despite the premise that there are many ways to build a successful CSIRT, a rough consensus was established in the forum on the steps that a CSIRT has to go through in order to be seen as a serious and trustworthy partner to other CSIRT:

a. Define what the role of the CSIRT in the community is;
b. Define what services/products the CSIRT is to produce;
c. The CSIRT has to convince its peers that b) is doable;
d. The CSIRT has to deliver on a) and b);
e. The CSIRT has to get data that make delivery easier;
f. By delivering d) the CSIRT gains more trust, and will receive more data from its peers and continue a positive way forward in cooperation, trust and effectiveness;
g. The process of gaining this trust can be time consuming, and there are few shortcuts to actively working and partnering with others to get to this point.

There are further opportunities to refine this methodology, for instance by discussing applicable laws, tools, guidelines and manners of cooperation. There is opportunity for multistakeholder engagement between CSIRT and their varied constituency to refine this model.

5. Unintended consequences of policy interventions, good and bad

Policy discussion

As it was discussed above, top down approaches from governments on creating CSIRT do not always work well. This has everything to do with trust. Assuming that governments and international governmental bodies mean well with their interventions and policy advice, there may be some lessons to learn here, e.g. that a CSIRT can only be successful when it adheres to certain preconditions, as mentioned above.

The creation of a national CSIRT is viewed as a good idea, especially taking into account the discussion about a CSIRT of last resort. However, if the goals for this CSIRT are not well defined and clear from the start to all those involved, it may drive this CSIRT to take on other tasks (as well). The result may not be what is called for at the start of this process. There are examples where this has gone wrong considerably for national CSIRT[19]. The discussion around this topic has not led to final conclusions and warrants further debate in a multistakeholder setting.

The forum agrees on the statements made that at the political level the work of CSIRT is not always (fully) understood. This can lead to policy created at government level that could actually be counterproductive for the work of (national) CSIRT. Also, there are several strong misconceptions on e.g. what a CSIRT is and does or does not do. Some common misconceptions include that they operate in an hierarchal structure towards each other (e.g. that an enterprise CSIRT reports incidents to a national level CSIRT), that an organization like FIRST or APCERT is the highest CERT in the world, respectively region (e.g. that all other CSIRT report incidents to FIRST or APCERT). This is not the case. In addition, there are misconceptions on the actual work of present CSIRT and misconceptions on tasks and efficiency.

The result in some cases is that new national centres are created. In some cases, these centres may report to national security or law enforcement institutions. While not necessarily inappropriate, this can in some cases seriously hamper cooperation with other CSIRT, while chances are that the work at hand is already being executed in a successful way by existing CSIRT.

The inner workings of a CSIRT may not always be clear to organizations setting or planning cyber security policy at a national level. Identifying better ways of defining good practices and standards on what CSIRT do, and advocating these to organizations setting policy would be useful to help improve this situation.

Cooperation and the development of CSIRT in different parts of government is an area where the forum sees potential for future multistakeholder discussion. Having a good understanding of what worked and did not work in a particular region or country could significantly contribute to the quality and outcomes of the debate in this area.

There is concern in the forum that special laws on data sharing and the resulting legal consequences of sharing data to the national CSIRT can actually lead to less sharing of data, simply because the "owner" of the data does not know what will happen with it. For instance, he could be fined on the basis of another law as a result of sharing or the data can be used as evidence in a court case.

CSIRT that have a close relationship with a regulator or law enforcement agency, or that have a legal duty to report to those, need to be particularly clear about the terms on which they can receive

[19] The forum decided on not to name and shame.

information and under which conditions they have to share data with LEAs. Other organizations may well be concerned that once they share information about incidents, this will trigger a regulatory or criminal investigation. Separating (possibly by law) the CSIRT's information-handling function from its duty to report or investigate may be essential to allow the CSIRT to participate in normal information sharing. Good examples of this include ENISA's work on incident reporting by telcos[20], the former UK National High-tech Crime Unit's Confidentiality Charter[21] and the arrangements under which regulatory agencies participate in ISACs.

Another interesting area of discussion is privacy. Strict privacy rules are meant to protect individuals' rights against collective might. CSIRT in many ways contribute to privacy, by ensuring incidents and data breaches are properly responded to, or even by educating their constituency on how to protect data. An interesting topic for further discussion is to determine in what ways privacy legislation affects the work of CSIRT.

6. Unresolved issues where further multistakeholder cooperation is needed

The forum feels that the discussion around national CSIRT and the CSIRT of last resort is ready to bring forward further discussion.

The forum expressed the need to open up to other communities in order to get a better understanding of the work of CSIRT on the one hand and the possibilities to cooperate better on the other. The suggested range of stakeholders is as wide as the topics discussed in this forum are.

Another area which is interesting for further debate, and in particular, for involvement of a more global community, is the cost of participation in international processes for developing countries. Examples from developing countries show that there may be a need for further debate and assistance to governments on what CSIRT are and what they could or should at a minimum do. Tied into this discussion is a debate around setting priorities and understanding the urgency of cyber security incidents, funding, schooling and the need for travel opportunities.

A question that could be explored further is the role CSIRT can have in solving the root causes of incidents and/or emergencies, such as in the prevention of cybercrime. If there is a desire to cooperate more, it is necessary to meet and discuss with other stakeholders involved. An example is the sessions that ENISA organizes once a year since 2011 between CSIRT and cyber crime units of the national police forces of the EU[22].

The CSIRT community needs to continue working with policy makers and the statistical community to improve the quality and international comparability of the statistics produced by CSIRT, in order to improve cybersecurity policy-making processes through better data.

In order to mitigate cybersecurity incidents, it often is necessary to share privacy sensitive data, i.e. IP addresses, between different (public and private) organizations. This is (perceived) as acting

[20] http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCEQFjAA&url=http%3A%2F%2Fwww.enisa.europa.eu%2Fact%2Fcert%2Fsupport%2Fincident-management%2Ffiles%2Fgood-practice-guide-for-incident-management%2Fat_download%2FfullReport&ei=QVUpVNTND9ffatGCgpAG&usg=AFQjCNGLQLIXe8F61nL1Qj_Ur-Jv_ij7xQ&bvm=bv.76247554,d.bGQ

[22] See e.g. this report: https://www.enisa.europa.eu/activities/cert/events/8th-cert-workshop-part-ii

contrary to privacy laws. There is a need to engage with the appropriate stakeholders and debate on solutions.

7. Insights gained as a result of the experience

There are several insights that have come forward from this forum that it would like to share at this point in the process.

a. There is a strong preference for the term CSIRT over CERT. This is the reason why the CSIRT abbreviation is used in this document.

b. There are different CSIRT within different organizations. Their goals, constituency and services may differ. However, all are involved in mitigating cybersecurity incidents or emergencies on behalf of its constituency. This constituency can be within their own organization and/or can be delivered to others outside of it.

c. The most important factor is that these CSIRT are able to work together, accept each other's information and deliver what they are supposed to.

d. In cooperation, everything comes down to trust. There is no legislation that can give trust to an organization. It is built up over time, time and again, with delivering what is needed and promised, in a timely fashion, and providing the security and adhering to the sensitivities needed for cooperation.

e. The success or failure of a CSIRT has everything to do with the correct determination of its deliverables, next to the perceptions of other stakeholders. Sometimes, success is not clearly defined, which contributes to confusion around whether the CSIRT is delivering or not.

f. The way CSIRT cooperate on the global, regional and national level on sharing knowledge, providing training facilities and actively work on trusted relationships has led to documents that are freely shared and available to all. These documents often describe a possible way to achieve a certain goal, rather than define a common practice which the community has converged upon.

g. Many CSIRT around the world mitigate incidents and respond to emergencies on a daily basis and are successful in their work. They do so in collaboration with many different partners. There are several formal and informal networks that have proven to be a success. However, these networks are not easily accessible to everyone concerned yet, due to regional differences in budgets and priority settings.

h. There is a clear need for a "CSIRT of last resort" in a country. It is not important who this CSIRT is, as long as its function is clear to all and it is able to act on request for assistance from third parties. In many countries this will be a national, governmental CSIRT, but, as examples show, it may also be a CSIRT operated by other stakeholders. The most important thing is that a CSIRT is able to coordinate any incident at a national level, when no other party involved is able to take on that role.

8. Proposed steps for further multistakeholder dialogue

One intended outcome is to make sure that challenges the CSIRT community faces are taken up and brought to the right stakeholder forum. This can be achieved e.g. by inviting other stakeholders to join CSIRT meetings and the other way around by sharing knowledge and laying contacts at meetings of other stakeholder's events.

The forum's leadership invites all stakeholders to join this discussion. The following topics are recommended for further debate in 2015.

a. Misconceptions of functions and tasks of CSIRT. Misconceptions lead to misunderstandings that can seriously influence the performance of a CSIRT and thus the performance of colleague CSIRT. Cooperation and the development of CSIRT in different parts of government is an area that needs further development and discussion.

b. The mitigation of incidents involves sharing (privacy sensitive) data. There is a clear identified need to discuss this topic further with governments and (privacy) regulatory agencies. (Perhaps in combination with other stakeholders facing the same challenge.)

c. National Point of Contact or CSIRT of last resort. The call to have such a point in as many countries as possible is evident. There is a need for further discussion on its functions and how to achieve this goal.

d. Privacy and free speech. Discussions showed that there are concerns in how far (the work of) CSIRT impede on free speech, as well as in what way CSIRT can contribute to a higher privacy standard in the world.

e. The implementation of good standards. There is a need for swifter implementation of Internet standards and good practices in general and at CSIRT in particular.

f. (Mandatory) cooperation with law enforcement and other regulatory agencies. Mandatory cooperation with LEAs tends to lead to a lesser trust between CSIRT. On the other hand, there is a possibility to cooperate more on a voluntary basis. This thin line is worth discussing further with other stakeholders involved.

g. Schooling, education and participation in international meetings. The importance of this topics cannot be underscored enough if a successful CSIRT is a nation's goal. Capacity building and CSIRT is a topic that needs to be brought further.

h. The development of case studies. There is a need for extensive case studies, such as on DNSChanger and Conficker, in the light of (the implementation of) lessons learned, potential cooperation with other stakeholders and reporting mechanisms in different jurisdictions.

In as far topics for further discussion or study were identified that solely involve the CSIRT community, they are, for obvious reasons, not included in this section.

List of contributors

Lead Experts:

1. Christine Hoepers
2. Maarten Van Horenbeeck
3. Adli Wahid

Contributors[23]:

1. Carolina Aguerre
2. Jaap Akkerhuis
3. Kossi Amessinou
4. Jerome Athias
5. Olawale Bakare
6. Simon Bang
7. Cem Barut
8. Jacques Beugre
9. Kamata Comode
10. Andrew Cormack
11. Patrick Curry
12. Tarik El Yassem
13. Nina Elzer
14. Asama A. Excel
15. Patrik Fältström
16. Patrick Green
17. Robert Guerra
18. Niel Harper
19. Kristo Helasvuo
20. Jahangir Hossain
21. Jean Robert Hountomey
22. Yurie Ito
23. Karen Johnson
24. Merike Kaeo
25. Keisuke Kamata
26. Olévié Kouami
27. Miroslaw Maj
28. Aaron Martin
29. Carlos M. Martinez
30. Thomas Millar
31. Kathleen Moriarty
32. Karen Mulberry
33. Bob Natale

[23] This list includes:
- the participants in the online discussions held via the dedicated mailing list;
- the contributors who commented on the online review platform (those who have not indicated their full names when making comments were not included in this list);
- panellists in the Best Practice Forum session held during the IGF 2014 meeting.

34. Michele Neylon
35. Seun Ojedeji
36. Rohana Palliyaguru
37. Damir Rajnovic
38. Shreedeep Rayamajhi
39. Robin M. Ruefle
40. Jordana Siegel
41. Andreas Schmidt
42. Baya Sylvain
43. Paul Vixie
44. MITA CSIRT, Malta Information Technology Agency

Editor:

Wout de Natris