Internet Governance Forum

Best Practices Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security (2015)

Executive Summary

The work of the Best Practices Forum (BPF) on Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security builds on the final report of the 2014 BPF on the same issue[1]. There is 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*". One overarching priority emerging from 2014 focused on addressing misconceptions around the role and responsibilities of a CSIRT. A brief investigation showed that the misconceptions are rarely within the CSIRT community, but arise in its interactions with other stakeholders. Among other things, they demand additional tasks from CSIRTs or embed CSIRTs in wider security organizations. This comes with intended or unintended consequences on trust, which could affect the relationship between CSIRTs. Valuable contributions were provided from different perspectives, including civil society, private industry and international organizations.

Major findings

This BPF showed that the role and involvement of CSIRTs in national security and/or guarding economic interests tends to expand. Change brings the need for direct involvement of CSIRTs in policy discussions and brings the traditional definition of a CSIRT under considerable strain. While the need to cooperate with other involved stakeholders could bring mutual benefits, it could also, as a downside, have a negative impact on trust within the CSIRT community itself. Trust is seen as an essential element facilitating mutual assistance and information exchange between CSIRTs. While the Forum was able to show several successful examples of expanding roles and new ways of cooperation, some concerns remained. There was a general agreement that communication between CSIRTs themselves and with other stakeholders is of vital importance to avoid misconceptions and maintain or gain trust and cooperation. Finally, it was recognised that responsible disclosure by ethical hackers is a topic that deserves further debate.

Participants in this Forum found its work very valuable. One indicator for the level of success is the fact that controversial topics within the CSIRT community were addressed in this BPF, and in some cases altered within the CSIRT community itself or successfully brought to other fora such as FIRST, OECD and the Global Forum of Cyber Expertise. At the same time, challenging topics were identified as laying

[1] http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-Internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file. The recommendations of the 2014 process are in Annex 1 of this report.

ahead, such as security incidents in the cloud, CSIRT maturity, CSIRT metrics, cooperation with LEAs, which merit future work.

The experts involved in the group felt there would be value in continuing the work. This could be done either in a third iteration of a BPF or by potentially widening its scope through forming a Dynamic Coalition dealing with the broader aspects of cyber security in a multistakeholder setting.

Suggestions for further work

The CSIRT community found the work carried out by this BPF to be of great value. The work of 2014 has proven to be a source of inspiration for creating a new CSIRT within a country. One tangible outcome was the creation of a CSIRT in Serbia. Furthermore, this BPF addressed topics that confront the CSIRT community with outside pressure on their way of thinking and working as it evolved over the past decades. Experts discussing these pressures concluded that core values have to be made known more universally and that a new way of cooperation and data sharing may be necessary in a fast changing world. CSIRTs now bring questions and potential answers to the table in different fora, including their own. The main recommendation of this BPF is therefore that the work continues in one form or another.

The particular, added value of the IGF is its role as connector. While there are many different institutions dealing in-depth with specific issues, the IGF has the potential of bringing experts from different stakeholder communities together in the search of common solutions. If the past two cycles of this BPF have shown anything, it is how influential such a process can be.

Therefore, this BPF does not consider its work completed. It sees a few different ways forward. Different options are presented to the IGF community for consideration.

Follow-up to the BPF 2015

a. A third BPF iteration

The work in progress, as described above, is seen as so successful and influential, that several experts in the BPF have indicated they want this BPF to continue, also because many new topics need to be addressed in a multistakeholder environment. These could include further work on themes such as privacy, data protection and transparency; the influence of CSIRTs on other stakeholders in the ICT (supply) chain, e,g, in botnet mitigation, the implementation of Internet standards and best practices, or more secure ICT products.

Among possible issues to be taken up by a new BPF, the experts identified responsible disclosure. Currently, this issue has gained a lot of attention in different fora. However, it would benefit from further discussions in a multistakeholder setting such as the IGF and should be considered for a new BPF in 2016.

b. Dynamic Coalition on cyber security and safety

Another way forward is currently being studied by those involved to deal with the broader aspects of cyber security. This could be done by forming a Dynamic Coalition involving experts who had been working together in the BPF on the 'Regulation and mitigation on unsolicited communications', as there are overlapping issues concerning cybersecurity and network abuse. Preliminary discussions focused on the theme "preventing network abuse". These discussions are ongoing. Questions that could be addressed include the following: how to reduce abuse; implement best practices and improve the overall security of the Internet?

Cyber security can only be realised when accepted, worked on and dealt with through the whole chain of parties involved, from software developers to infrastructure providers and incident response teams. Many of those directly involved are missing in debates as those taking place at the IGF. This is an issue area that would benefit from the multistakeholder approach and could be taken up by the broader IGF community in different formats, such as a BPF, but also main sessions, workshops, national and regional IGF initiatives. This Forum recommends investigating these wider aspect of cyber security next.

General recommendations

This work cycle has led to new insights that have been captured in the following recommendations for the CSIRT and other communities.

Recommendation 1: There is a need for policymakers to discuss the role of CSIRTs with the CSIRT community to avoid misconceptions around the role of CSIRTs.

Recommendation 2: CSIRTs are recommended to be actively involved in relevant policy discussions at both the national and international level. In order to engage with other stakeholders, it is important to be where they are. The provided examples show that it brings influence and understanding.

Recommendation 3: Every government has the right to create the CSIRT it needs. It is recommended though that governments make an informed decision, taking in the potential consequences of their choice.

Recommendation 4: Where CSIRTs are concerned privacy and security have to stand together in order for a CSIRT to be truly successful.

Recommendation 5: It is advised to use the term 'data protection' in a CSIRT context more as it is far more concrete and better understood than 'privacy'.

Recommendation 6: Data protection has to be at the core of the work of a CSIRT.

Recommendation 7: It is recommended to involve Data Protection Commissioners more in the work of CSIRTs.

Recommendation 8: To ensure transparency and accountability where privacy is concerned, it is advised to make a study whether a standard protocol can assist attaining transparency, as well as more conscious decisions about limits to data sharing, anonymization of data where possible and the handling of data by CSIRTs.

Recommendation 9: CSIRTs should minimize data collection and processing, while also focusing on their constituency and anonymizing relevant information.

Recommendation 10: A well-run CSIRT is an essential part in the protection of data and security within a society.

Recommendation 11: Further study is recommended into the expanding role of CSIRTs. This could e.g. include whether there are sensible limits to tasks given and what role a CSIRT can play in enhancing cooperation in the security chain between other stakeholders, e.g. manufacturers of ICT products and providers of ICT services and does the current definition of a CSIRT match the reality of work asked and tasked.

Recommendation 12: Further study is recommended into the ways CSIRTs and law enforcement can enhance their cooperation in meaningful ways, each from within its respective mission.

Recommendation 13: CSIRTs have a role in handling effects of cybercrimes and providing technical support for investigations, but cybercrime is overall crime and as such should be dealt by law enforcement entities, like the police. Containing too much of this work within a CSIRT, or making a CSIRT part of a law enforcement agency is likely to have significant impact on its ability to work with private sector.

Report

Introduction

This is the final report of the Best Practice Forum (BPF or "Forum") on 'Establishing and Supporting Computer Security Incident Response Teams (CSIRTs) for Internet Security (2015)'.

This report covers the work of the BPF, and as such refers to "this Forum" as comments which came out of the working group and the session in João Pessoa. The report reflects the input delivered to the BPF in combination with the research conducted on behalf of the report. It was in no way meant to be limiting and the group welcomed feedback, discussion and engagement across the IGF community and beyond.

The Internet is a global phenomenon, and the topic of cyber security is being addressed by a community of incident responders, policymakers and others across the world. This group can only be successful by developing trust and community between these actors, both inside and outside the IGF community.

This work builds on this BPF's work in 2014, when the IGF organized a Best Practices Forum around the topic of CSIRTs to find current best practices and to identify challenges the community faces. This led to a report published on the IGF website in 2014. The detailed recommendations in the report and the necessity to involve different stakeholders in future actions has led the Multistakeholder Advisory Group (MAG) to agree on a continuation of this work and provide more in-depth analyses and solutions to the challenges at hand.

In the past months the Forum discussed how to continue its work in meaningful and additional ways. This led to consensus on one main, overarching, theme:

"Misconceptions around the role and responsibilities of a CSIRT".

There is consensus in the Forum that this topic will cover many of the challenges[2] identified last year and was deemed most important to continue in 2015. It was divided into subthemes, but also brought alight new challenges that will be described below. Other themes identified in 2014 have to be discussed and have been discussed outside of this Forum, e.g. within FIRST or other relevant conferences.

With this choice comes the necessity for other stakeholders, outside of the CSIRT community, to get involved in this discussion and a different set of questions that need answers. A brief

[2] The recommendations of 2014 are found in annex 2 to this report.

investigation showed that the misconceptions are rarely within the CSIRT community, but do apply in its interactions with various other stakeholder communities.

As last year's report extensively shows, the definitions of a CSIRT have been established over the years and have been used successfully by the CSIRTs built ever since. This implicates that the misconceptions are elsewhere. One reason for misconceptions could be that certain stakeholders have demanded additional tasks from CSIRTs that go beyond the traditional tasks and are met with distrust from the "older" CSIRTs. In cases like these the constituency of a CSIRT may have changed, as well as in some cases its relationship with other CSIRTs. There could be distinctions between these changes for government, academic or commercial CSIRTs.

On this basis the Forum decided to do extensive outreach to those involved from different angles: Governmental organizations, privacy advocates, NGO's and supra national organizations. Online responses were limited. This led to a valuable lesson learned: CSIRTs need to engage and/or reach out more actively in order to be heard. This report will provide successful examples of new forms of cooperation and outreach.

Finally, that the work of this Forum can have unintended, but pleasantly surprising outcomes, is shown by the fact that the recommendations of last year's report were used as input for the building of a CSIRT in Serbia. The usefulness of this body of work was confirmed in the BPF CSIRT session in João Pessoa.

The BPF would like to take this opportunity to thank the many individuals who dedicated their time and knowledge working towards this report.

1. Definition of the issue

The idea that there are general misconceptions on what a CSIRT is and more precisely around what it does is widespread within the CSIRT community. The effect of these misconceptions or of the actions taken by "others" on the basis of these misconceptions is the loss of trust. This directly affects the effectiveness of CSIRTs as they exchange information and assist each other during incidents and emergencies on the basis of that elusive term "trust". As trust is a very personal quality, rather than provide prescriptive guidance on how to develop it, we are more likely to be successful at describing conditions in which trust is fostered. The range of options is literally as wide as having legal agreements specifying standard protocols, to having an informal talk together at a conference. Trust starts with personal relations and is maintained through the reliable delivery of services when a request is made. Nothing much will replace these conditions. No law, no directive, no best practice document can really take its place[3].

[3] Who, What, Where and How. An Insider's View to Participating in the Security Community. Presentation by John Kristoff of Team Cymru at FIRST (2012). http://www.cymru.com/jtk/talks/first2012-community.pdf

This Forum has reached consensus on the fact that different CSIRTs not only serve different constituents, can be embedded within different organizational forms, but also can have very different tasks. As one participant defined it: "*The role of CSIRTs is defined by the parent organization and CSIRTs should perform duties as they are given to it*". As a result a CSIRT could function within the military, a university, a company, a regulatory office, an anti-terrorism organization, etc. What complicates matters is not only the informal exchange of data that becomes harder, there may be totally different laws involved. The same goes for the thought of a "neutral" CSIRT. Every CSIRT has a constituency and is financed by an organization, which makes true neutrality hard to achieve.

Recently the topic of cyber war has risen to more prominence. Richard Stiennon's book[4] covers this topic, as does Bruce Schneier in an interview titled 'We're in early years of a cyber arms race'[5]. This Forum points to these publications because it leads to an important question: What is the role of a CSIRT in a politically motivated hack, a cyber conflict or worse? Schneier states that current targets are not nations' vital infrastructures, but companies, what he calls "soft targets". From his personal point of view he provides the example of the Sony attack on which he is quoted: "*Many of us, including myself, were skeptical for several months. By now it does seem obvious that it was North Korea, as amazing as that sounds*" [6]. He mentions Stuxnet as an example of how hard it is to prove who is behind an attack or intrusion[7].

Given the fact that nowadays nation states aggressively use vulnerabilities in software or defense systems of the attacked party, public and private, CSIRTs become automatically involved to some degree. Any organization, with or without a CSIRT at hand, becomes involved when under attack or is intruded and will need to cooperate with (other) CSIRTs and security companies to mitigate the attack or intrusion.

The EU NIS directive even obliges critical infrastructure organizations to report cyber incidents. The question may be whether this is enough, taking the almost daily disclosure of privacy sensitive data on the Internet through hacks of systems. This is reiterated by Mark Goodman in his book Future Crimes[8]. "*This silence [i.e. not reporting incidents] is at the very heart [of] our cyber-security problems*", he states. The result being that: "*these incidents cannot be aggregated and studied, common defenses are not developed, and perpetrators roam free to attack another day*". Goodman advocates that admitting a cyber problem is the first step towards getting better[9].

[4] There Will Be Cyberwar: How The Move To Network-Centric War Fighting Has Set The Stage For Cyberwar. R. Stiennon (2015)
[5] We're in early years of a cyber arms race, Neil McAllister (2015) http://www.theregister.co.uk/2015/08/19/bruce_schneier_linuxcon/?mt=1440182295531
[6] Ibidem
[7] For Stuxnet read: Countdown to zero day. Stuxnet and the launch of the world's first digital weapon. Kim Zetter (New York, 2014)
[8] Future Crimes. Mark Goodman, New York (2015)
[9] Ibidem, pp 374-375

In what way are incidents or emergencies like these responsible for the way CSIRTs are viewed from outside its own community? Do incidents like these give rise to view it differently? But also, what are incentives to report incidents and emergencies?

The issue of misconception displays a lack of trust in (the intentions, ideas or actions of) "other entities" of which the basis could lie in many factors. Many questions come with this theme, some of which are not always addressed in a direct way. In certain cases, negative ramifications may be perceived when addressing these uncertainties directly. However, these are questions that need to be addressed in order to create a basis that may restore confidence in each other and the "other entities".

Fact is that the exact roles of a CSIRT are a prominent concern of many governments, CSIRTs and international organizations - a prime example being the OECD report on CSIRT statistics[10] . A whole chapter, aimed at policymakers, focuses on what a CSIRT is, before it turns to the main topic of the report. The Global Public Private Institute published a paper in April 2015 called 'CSIRT basics for policy-makers. The history, types & culture of CSIRTs'[11] which was co-sponsored by the European Commission and the Netherlands Ministry of Foreign Affairs.

This Forum agrees that this is a sound approach, something which was widely supported as well during the session in João Pessoa. If CSIRTs are involved in more general policy debates, they can inform policymakers on their respective strengths. This way more people learn, directly from participation and indirectly by reading.

An anecdotal account from one country's participant illustrates that there can be deep mistrust between the (commercial) organizations, that would benefit from cooperation with a given national CSIRT, and the CSIRT itself. This stems from the fact that in this casus, the national CSIRT works under the office of the national security advisor. This office is aligned with state security and law enforcement. This approach appears to be common across Africa, and much of the developing world. While not necessarily ineffective, it does raise questions on the best methods of developing trust between a CSIRT and its constituency in this type of alignment. Private sector CSIRTs, as well as citizens, may be less willing to share when their data is used for enforcement and prosecution, rather than simply to mitigate incidents.

Of course, each government has its own reasons for positioning a CSIRT in a particular way. There is room to improve the overall trust situation by identifying the common rationale behind CSIRT development, and understanding which relative level of distrust appears in each model.

It was pointed out from a private stakeholder's point of view, that in order for a CSIRT from the private sector to share data with a national or other governmental CSIRT, it is often a

10 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282013%299/FINAL&doclanguage=en

11 http://www.gppi.net/publications/global-Internet-politics/article/csirt-basics-for-policy-makers/

requirement that it remains in a civilian agency responsible for protecting government and protecting citizens and not for conducting surveillance.

National CSIRTs were discussed extensively in last year´s report. As one contributor sums up this year: "*There is no right or wrong about who hosts a National CSIRT, or which services it should provide. From experience, each country will need to identify what works best in its case, as well as consider other issues like services, funding, local Internet governance structure and cultural issues, among other factors that might impact the decision*".

There is consensus that a government has the right to determine its own best implementation. If it reaches its own objectives, then it could be considered a success domestically - except for the fact that it may not reach objectives that it could have reached in different circumstances. In addition, the international integration of the CSIRT may be negatively affected by particular design decisions. There may be serious unintended effects or even well calculated effects on cooperation. It is important that government and policy decision makers are aware of these ramifications prior to making these important decisions, and the Forum sees a role for the BPF effort to contribute.

It all starts however with what a CSIRT is, what it does, for whom and with what. These topics were comprehensively addressed last year[12]. For now we will suffice with the given description of a 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.[13]"

Reading it, it shows how careful this description is given: "there is consensus". It suggests that there could be some dissenting opinions who have agreed to abide and those who decided not to live by it or have never been involved in the process. This is different when the Forum discussed what a successful CSIRT is. No one single answer was given. The misconceptions must stem from the difference from the consensus of those involved in the Forum and those outside having different interpretations and views.

For one, this situation is not unique. Several national CSIRTs work within broader organizations with different tasks, tasks that may be in conflict with basic functions of CSIRTs. It is of utmost importance, so it was advised in the Forum, to separate these broader functions from the CSIRT function and that those in management positions understand why separation of functions is necessary. This helps clarify what happens with data shared and allows us to measure whether

[12] Idem, pp 4 -10
[13] Ibidem

notable positive results come from sharing, which makes cooperation valuable and builds trust. There are some rules from experience that can assist in building a relationship that works:

- Have a published agreement for how you will (and will not) use information shared with your CSIRT function;
- Demonstrate that you can share information outwards too;
- Be clear and realistic about what information you can use, what you'll use it for, and how that benefits the organization sharing it with you;
- Make sure you demonstrate that sharing information with you was useful;
- Laws and regulation, as well as certification of organizations and individuals, while not in itself sufficient to help develop trust, can still be useful to make the behavior of a CSIRT more predictable.

This mix of measures is a combination of a formal solution (a signed and published agreement) and informal ones that show good faith and usefulness and can be a basis from which discussions start. If partners show that they are willing to comply to these rules, there may be a basis to tentatively start preparing for cooperation. On the other hand, distrust may be justified in some cases and the question to ask oneself in such a case is whether there is a CSIRT or another entity at the table?

This is explained more closely in the blogpost 'Government CERTs and Information Sharing'[14]. If CSIRTs have different functions, e.g. investigative and/or enforcement or resort under a special firm or a different law, information sharing can become harder or even prohibited by law. This leads to very different questions that go well beyond "do I trust you (or not)"?

This Forum has to look at in what ways have governments, in trying to find ways to make the Internet a safer place, started to redefine what it needs a CSIRT for. This may well conflict with older definitions of CSIRTs. When a governmental CSIRT, from protecting government networks scales up to being (seen as) a major digital defense line in protecting a country, tasks change accordingly. What are the consequences of this policy change and are these consequences fully understood or unintentional?

That governments and other CSIRTs, in the EU, are meant to step up efforts is shown by the intentions of the NIS Directive: "*The aim of the proposed Directive is to ensure a high common level of network and information security (NIS) across the EU*". Not only national CSIRTs are addressed, anyone operating critical infrastructure is obliged to step up their efforts, including the requirement to "*report to competent authorities incidents with a significant impact on core services provided*" [15].

[14] https://community.jisc.ac.uk/blogs/regulatory-developments/article/government-certs-and-information-sharing
[15] http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and , accessed 18-06-2015

This may indicate a clash of cultures. On one side there are demands for protection of economic and national values and on the other the traditional, more libertarian Internet community which values the freedom to tinker and trial new technologies. Beyond that it may (also) be a point of disagreement with the intelligence services and the military. Misconceptions are high between the two, but as someone observed, stating: "*politicians and lawyers should leave CSIRTs alone, they know what they are doing*", when directly asked for input, is not helpful. To have a safer Internet experience through less threats and incidents is the main driver for all involved, so are there ways to meet on mutual ground and work together from there?

Set of questions
In order to interact with other stakeholder communities this BPF found that a different set of questions needed answering. If it is necessary to interact with these stakeholders in order to be able to keep working as the CSIRT community is used to, it is necessary to identify more specifically what is exactly at stake, what and who causes a lack of trust through misconceived actions. So e.g., who are these "other entities" the CSIRT community addresses? What are their actions and what makes these actions lead to losing trust in sharing vital information in mitigating incidents and emergencies?.

Over the months another question became apparent to the Forum: "How do we engage other stakeholders?" All were actively invited to share their ideas on how to proceed with the topic of misconceptions. This can be divided into several sub-themes.

Sub-themes
CSIRTs and privacy
From outside the CSIRT community it can be said that there is consensus on the fact that the work carried out by CSIRTs is conceived as positive. Comments were made that where privacy is concerned, CSIRTs could operate more transparent and make conscious decisions on what set of data is shared under which circumstances. When are anonymized data sufficient and when not?, is a relevant question put to the CSIRT community.

That said, the internal discussion led to some interesting insights. CSIRTs work with privacy sensitive data on a daily basis. For instance by learning about compromised computers and ultimately identifying its network owners to allow for remediation.

The question is how to use the data, process it, notify those involved, what to share with other CSIRTs and stakeholders involved? In all these actions there are decisions involving data protection (law). There is consensus between those involved in the online process of this BPF that security and privacy go hand in hand and that CSIRTs work continuously to protect the privacy sensitive data of their constituents, on a daily basis. In fact the question is put slightly different, within the CSIRT community: "*How are you going to protect privacy and free speech on the Internet *without* a CSIRT to let you know when a malware strain is exfiltrating private*

data, or who will assist when a (D)DoS attack floods your preferred communications server with unwanted traffic? Neither of those can be done by the end user".

This is part of the misconception of the work CSIRTs do, so the CSIRT community argues. Could this be altered by producing a paper "with explanation about what kind of information could be given and under which circumstances?" Confusion is exacerbated as there are so many different law and privacy regimes under which CSIRTs operate. Two other questions were brought forward that may assist in bringing the discussion closer to a satisfactory end:
- What privacy best practices should/could CSIRTs adopt and implement?;
- What role (if any) can/do CSIRTs play in prevention, mitigation, recovery from incidents involving data breaches?

This comes forward also in the preposition that privacy is often in competition with security. It ought to be the other way around: privacy and security stand together and CSIRTs are a key control in achieving them. This is a principal argument in the debate within the Forum. It was argued that some entities go beyond security and want to implement control mechanisms. These same entities spread the claim that it is hard to have security if privacy measures are in place. In other words the outside debate focuses on control vs. privacy. It is obvious that trust issues between these entities and CSIRTs are at play.

One solution could be that the term "privacy" has to be abandoned from this debate. Privacy is subjective and means something different to many people, jurisdictions, etc. Data protection, including protecting the confidentiality and distribution of sensitive information, is easier to define in law, so a better term to use for this Forum as well. It was noted that when addressing the public at large, the term "privacy" is better understood, because this is what end users worry about. There is consensus in the Forum that data protection is one of the roles CSIRTs have. It seems important to involve Data Protection Commissioners in the debate. It was noted that they often support the work of CSIRTs.

At the heart of the matter stands that there is no common data protection law around the world. On top of that judiciary regimes are quite different. This complicates any debate on the topic. The strictest privacy law arguably comes from the European Union. This Forum received an article called 'Incident Response and Data Protection' by Andrew Cormack[16] on the decisions that EU CSIRTs should consider or make on the basis of the Privacy Directive[17]. The Directive permits the kind of processing that takes place at CSIRTs, "*provided certain conditions are met. The paper identifies these conditions and suggests measures that CSIRTs may use in planning and performing their activities to satisfy the requirements*". It looks at the matter from several angles and topics and provides potential ways forward. Being from 2011, it may have lost some

[16] https://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf It is Andrew Cormack's intention to work on an updated version later this year.
[17] Directive 95/46/EC

of its actuality as the Privacy Directive is about to be renewed and in some instances becomes stricter. The good side is that the work of CSIRTs is explicitly mentioned in the Directive:

"The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams –CERTs, Computer Security Incident Response Teams –CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. ..." [18] and:

"*...This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."* [19]

The contribution from the European Commission to this report underscores our findings:

*"Privacy in itself (is) not a limiting factor for the work of CSIRTs, as there are regulatory clauses in the legislation (*at least in the EU*) which allow CSIRTS to perform their work (incident response, forensics, log analysis) and access private data for the purpose of securing the networks. As for the cooperation with the wider community, in sharing information on vulnerabilities or threats the information can be anonymized and there is in most cases no issue of privacy either".*

Andrew Cormack presented on three sensible steps to follow before processing data as a CSIRT:
1) Concentrate on constituency;
2) Minimize data and processing;
3) Think about information flows[20].

[18] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
[19] Draft General Data Protection Regulation, Recital 39
[20] Protecting privacy through incident response. A. Cormack. (https://community.jisc.ac.uk/blogs/regulatory-developments/article/protecting-privacy-through-incident-response) accessed 22-8-2015

In more practical terms this comes down to choices to be made between the necessity of investigation of a threat against the privacy of the individual. A conscious choice or "*a balancing act*", as he calls it, between the two, assists in providing legitimacy for the ongoing work.

The comments provided from outside the CSIRT community point in the same direction. Transparency and accountability become part of the discussion. The posed question on when is what data shared and is it necessary to share is a valid one. It is recommended that CSIRTs minimize data collection and more importantly the processing of that data. CSIRTs could work in a more transparent way if a (policy) document was published that provides information in a general way, which makes this part of the work more transparent and accountable from a privacy point of view.

At this point in time there is no final text of the new EU regulation on privacy, this is expected for the end of 2015, with a two year period for implementation for the Member States. Fact is, the work of CSIRTs is fully recognized and supported under (to be) set conditions. It is these conditions that need to be crystalized. This could take the form of guidelines or best practices.

Incidents, threats and attacks come from/take place beyond the EU as well. There is a need to get to know what the best practices or common standards here are.

A concern was raised from a human rights point of view. What is missing is a text supporting human rights defenders. Regulatory clauses in the legislation which allow CSIRTs to access private data for the purpose of securing the networks create a very thin line that can be crossed and misused by oppressive regimes. A statement by CSIRTs concerning human rights would be much welcomed.

In conclusion, it is important to understand for all those directly and indirectly involved that "*a well-run CSIRT is an essential part of protecting their privacy and security*".

Policy and CSIRTs

Part of the misconception debate focuses on the misconceptions that policymakers have concerning the work and tasks of CSIRTs. A good summary of these tasks is provided in the recently published OECD report "Guidance for improving the comparability of statistics provided by CSIRTs"[21]. It even specifically aims at preventing misconceptions: "*Those sections were largely intended for policy-making audiences.*" One of the reasons the report was written, is the following: "*Policy makers are increasingly interested in reliable, trustworthy information about current and historical cybersecurity trends and the effectiveness of digital security risk management measures ("security measures"). Due to CSIRTs' unique role in the digital ecosystem, there is mounting interest in CSIRT-produced statistics to inform policy making in the*

21 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG%282013%299/FINAL&doclanguage=en

area of cybersecurity." In other words, it is extremely important what policymakers can expect from CSIRT.

The question could be in how far not only the future work of this OECD working group could be used in further debating misconceptions. The infrastructure between policymakers and CSIRTs is there, the basic work has been done. The OECD understands the importance of CSIRTs and why misconceptions are to be avoided. The question should also be in which other policy processes could CSIRTs successfully contribute and influence opinions?

In its contribution the European Commission points to the fact that national or governmental CSIRTs are in regular contact with policy makers. On influencing policy it states: "*In general terms a country level CSIRT can indeed influence policy by bringing to the attention new threats, new techniques and vulnerabilities and highlight the need (if any) for additional regulation or coordination*". The Commission also points to the fact that policymakers have acknowledged the role of CSIRTs in national cyber security strategies and refers this Forum to publications by ENISA and NATO/CCDCOE.

(Supply) chain approaches to cyber security and the role of CSIRT
The security and safety of the Internet is becoming a major concern for all stakeholders. If it isn't yet, it will be soon. CSIRTs play a major role in creating a safer and more secure Internet. The concept of a (supply) chain approach, where all manufacturers of ICT (components) and service providers take a specific role of implementing distinct cyber security measures applicable to their service, is regularly discussed in different fora. In particular, the success of botnet mitigation solutions, a topic many CSIRTs and other stakeholders are involved in, depends on active participation within the whole chain.

The question was posed whether CSIRTs could play a more active, perhaps even leading role in addressing this approach. Case studies were received from Switzerland and the Republic of Korea, where active and steering approaches have been chosen[22]. Where SWITCH acts more proactively towards third parties, KrCERT/CC maintains a number of services that are comprehensive and support their constituency in novel ways, which are not common across the CSIRT community.

An article by the Delft University of Technology[23] underscores the concept of potential influence within the chain. It shows that having an anti-botnet initiative within a country is only one line of defense against, in this specific case Conficker, malware infections. This is a conclusion to be expected. Disinfection mitigates the result, but does not affect the root causes. In the longer term cyber development and capacity building will assist countries with higher infection rates due to a higher use of pirated software. The article continues: "*The strong correlation with software*

[22] The case studies can be found in Annex 2 and 3.
[23] Post-mortem of a zombie. Conficker Cleanup After Six Years. H. Asghari, M. Ciere, M. van Eeten (Delft 2015). https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/asghari

piracy suggests that automatic updates and unattended cleanups are some of the strongest tools in our arsenal. It supports policies to enable security updates to install by default, and delivering them to all machines, including those running unlicensed copies"[24]. As the article professes, most infections come from illegal or pirated software. This is one example of how changing relations or conditions within the supply chain could assist in securing the Internet.

Of course there are many other root causes. Questions that still need answering are the following. What roles do CSIRTs play currently and are there roles foreseeable in the current mission of CSIRTs that can make a difference but perhaps (are under-)used? What examples are there of CSIRT working with the supply chain for a higher level of security and safety?

The two case studies at a minimum show promise for new roles for CSIRT and to provide extensive, non-standard services to their constituency which materially improve cyber security. The BPF recommends further debate and study into this topic.

Case studies
- ENISA CSIRT – LEA cooperation program

One of the instances where misconceptions on the work of CSIRT come to light is in cooperation between CSIRTs and Law Enforcement Agencies (LEAs). ENISA has a program that runs now for a few years, in which the two stakeholder groups meet and learn about each other, the work carried out and search for ways that they can cooperate. The program is aimed at a better understanding and the building of trust between the two stakeholder communities. One of the participants gave an overview of the current state of affairs:

- *"CERTs traditionally combat the effects of cybercrime: They help customers, i.e. their constituency to quickly recover and resume normal operation after an incident. CERTs typically work informal and with ease across national borders. Law enforcement agencies (LEAs) on the other hand are mostly interested in finding and prosecuting miscreants. LEAs are bound to strict procedures and find it difficult to collaborate across borders.*
  It has been suggested, that CERTs could bridge the international gap to make Law enforcements more effective, or even "take over" some of its jobs.
  This is not working: CERTs do not have the authority to conduct police investigations, and it's not their job either. Rather a meaningful collaboration between CERTs and LEAs has to be established. This has been recognized by ENISA for quite some time. Since 2015 joint workshops have been organized to foster this collaboration. WPK 4.1 in the 2015 ENISA Work program aims at exactly this: "WPK 4.1: Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS".
  The process is a slow one though, due to the different cultures and the legal framework governing LEAs and CERTs. Specifically:

[24] Ibidem

- *CERTs and LEAs often don't share the same vocabulary. ENISA is now developing a common taxonomy to solve this issue;*
- *LEAs and CERTs cannot share information symmetrically. This often causes great frustration among CERTs as the police may not share information in ongoing investigations.*

Here I feel CERTs just have to accept this:

- *Much of the information obtained by CERTs may not be usable in courts;*
- *The place of the crime is not where the damage occurs: Thus no LEA feels responsible;*
- *Just having LEA on board is not enough, also prosecutors and possibly judges need to understand the issues and the ways CERTs work.*

SWITCH-CERT in Switzerland is working closely with law enforcement to address and explore these issues, so possible solutions can be found. But just "throwing a CERT at it" is not solving any problems. Unfortunately there are still many politicians and (mostly national) CERTs which just claim exactly that.

Misconception: CERTS will solve the problem of cybercrime. Fact: CERTs play an important role in fighting cybercrime by supporting the authorities doing their job, but not taking it over. [25] *"*

The Switch contribution is underscored by the European Commission:

"Most CSIRTs do not have a legitimate law enforcement function. In fact, they benefit from not having such a function because it lowers the threshold for individuals and organizations to report incidents and ask for help. However, most CSIRTs have a frequent cooperation with law enforcement as a technical support function to investigations".

This particular misconception is encountered in cyber capacity building programs around CSIRTs in developing nations. It is seen as highly important that policymakers in these countries understand the distinction between a CSIRT and law enforcement. It is advised that mechanisms to discuss this topic are built into the capacity building programs.

Despite the fact that misconceptions are noted, experience shows that law enforcement and CSIRTs do enhance each other's roles by lending knowledge and expertise to each other when and where necessary, supported by a clear understanding of their respective roles. CSIRTs have a

[25] Contribution by Serge Droz, SWITCH-CERT, Switzerland

role in handling effects of cybercrimes and providing technical support for investigations, but cybercrime is overall crime and as such should be dealt by entities like the police.

- Regional specificities observed

Some of the questions asked to the Forum aimed at identifying differences between regions. It proved hard to get beyond common observations. Yes, differences in cultures and jurisdictions will show differences in how a CSIRT is tasked and organized. The most safe, but rational conclusion was that a CSIRT will do what it is told to do, region notwithstanding.

What was pointed out also, mostly in contributions from developed nations, was that the problems faced in developing nations are different in many cases from developed ones. There are problems with e.g. (a weaker) infrastructure, financial issues and the need to justify the work done in the face of an unknowing nation. This makes it hard for a CSIRT to mature. Overall, it became clear that many factors play into the success of a CSIRT, and it is difficult to generalize across a region, let alone the world.

An issue like under-funding may not be a regional specificity per se. So a difference between well-funded CSIRTs and less or under-funded CSIRTs could be justified here. All agree that sufficient funding is one of the basic ingredients that make a CSIRT function. For the others resourcefulness is the advice given. An example provided was that of volunteers coming together during an incident to assist, and later needing to find funding sources to make their effort "stick".

- Existing policy measures and private sector initiatives, impediments

At the Global Conference on Cyber Space (GCCS) 2015 the CSIRT Maturity Toolkit[26] was presented[27]. "*The purpose of this CSIRT Maturity Kit is to help emerging and existing Computer Security Incident Response Teams (CSIRTs) to increase their maturity level. This is achieved by offering a set of best practices that cover CSIRT governance, organization and operations*"[28]. As such it is one of the initiatives within the Global Forum of Cyber Expertise that was launched during the GCCS 2015[29].

- What worked well, identifying common effective practices

The involvement of CSIRT representatives in policy discussions proves to be influential. The examples this Forum was able to provide, clearly show that CSIRTs and thus CSIRTs' role, can only be heard when voiced in policy discussions.

[26] https://www.gccs2015.com/sites/default/files/documents/CSIRT%20Maturity%20Toolkit%2020150409.pdf
[27] https://www.gccs2015.com/nl/csirt-maturity
[28] Ibidem
[29] https://www.gccs2015.com/gfce

Despite the fact that not all participating in this Forum see a role for CSIRTs with/in law enforcement at all, others have indicated they do see a role, but mainly on the condition that the roles are truly and correctly separated. Both have their own role and within this role CSIRTs can assist LEAs with building evidence, e.g. through providing technical expertise or analyses of complex attacks. Another way could be by providing information found. This is one of the main topics of the ENISA initiative discussed earlier and something that may prove effective. Discussing difficult topics often provides mutual understanding and helps to build trust to find solutions where these were unheard of before. Future work could focus on identifying cases where this collaboration took place with a successful outcome.

In the fight against infected machines (bots) the example of Finland[30] and more recently of Switzerland shows that a pro-active stance of CSIRTs, in Finland backed-up by law, lead to diminished rates of infections, also making the country less attractive to target from an infection point of view. Quick disinfections are discouraging for criminals. It makes other countries safer as well.

The private initiative in the Netherlands against Distributed Denial of Service (DDoS) attacks called Nationale Wasstraat ('National Scrubstreet') is a private initiative that claims to work well[31]. A similar, but public, example can be found in the Republic of Korea's National DDoS shelter as presented in Annex 3.

CyberGreen

CyberGreen seeks to aggregate data and provide metrics to measure risk conditions globally through collaboration and data sharing partnerships. National CERTs are partnering with CyberGreen to share and consume risk metrics. A central goal for CyberGreen is to assist policymakers in identifying areas of the Internet that need additional attention and resources due to their risk conditions. CyberGreen would partner and assist the existing organizations that play a significant role in remediation efforts such as cleanups, botnet take downs and identifying and remediation of vulnerable nodes. National CERTs and Network operators are encouraged to sign up and explore CyberGreen's portal to give CyberGreen guidance and feedback on what would most help for CERT engage their policy makers[32].

CyberGreen is in need of funding in order to carry on its work.

[30] http://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/411-bpf-2014-outcome-document-regulation-and-mitigation-of-unsolicited-communications-spam, p 11, 12

[31] NAWAS case study, 18-08-2015

[32] http://stats.cybergreen.net/

- Unintended consequences of policy interventions, good and bad

Misconceptions are at the basis of this BPF's draft report. There currently is consensus that the implications of stakeholders adding new functions to the CSIRT function is a danger to the traditional and successful way of collaboration on a trust basis.

What is hard to conclude on at this point in time is whether these measures are an unintended or an intended result, in as far that this result was calculated at the time of decision making. In order to draw this conclusion more information is necessary. Thus it becomes more an unresolved issue.

Serbia case study

After the IGF secretariat published the report on CSIRTs in 2014, it was used as a background document for the local capacity building project and discussion on cybersecurity in Serbia. The adjusted summary of the document translated into Serbian was also added to the final booklet of the project[33]. This shows how the Forum's work can be of influence in policy debates and can be noted as a tangible outcome of this Forum's work in 2014.

- Unresolved issues where further multistakeholder cooperation is needed

A clash of cultures?

There is a general feeling of distrust in the CSIRT community about "actions" of "other entities". The CSIRTs that are in place for some years now were built under the current examples of how CSIRTs were defined in the past 20 years. With the interest of other governmental agencies and ministries in the Internet and the importance to which the topic has risen for the economy and with that the national security of nations, the entities and people interested in the work of CSIRTs have significantly changed. With that the idea of an "Internet free state", the concept of permissionless innovation and the libertarian, government free state of the Internet have all come under pressure and are challenged. At the same time CSIRTs, as brought forward in the Forum, have a tendency to shy away from policy making. On the other hand, in a 2015 FIRST initiative, the organizations participating did identify "cybersecurity policy advisory" as one of the new roles of a CSIRT, so there is some indication that the community does have an interest in contributing to policy as it is developed.

It was suggested that CSIRT metrics could assist in clearing up misconceptions, if these metrics can show what or which CSIRT actually works well and what/which one does not.

At this point in time a clash of two, but most likely three cultures is taking place in which the traditional way of working of CSIRTs is challenged.

[33] http://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez

On the one hand there is the government which aims to increase the role of CSIRTs where they take on a crucial response capability for the wider nation, often with some tension to involve law enforcement and the intelligence function. There is the technical community which wants to ensure its role is limited to those response capabilities, enabling it to work effectively with other CSIRTs that have similar roles. On the other hand, companies with (vital) national interests often of a private nature have become prime targets. This brings that they are looked at differently from a security perspective. Their CSIRTs, if they have one, are in the front line and most likely have gained in interest from higher management levels as well.

Experience shows that the informal way CSIRTs work together is a major driver of their success and increased bureaucracy may make this informal cooperation less effective.

Does all this bring the need with it to become involved in policy making? Or is it already more common place than this Forum thought at the start of this work cycle? From the Forum discussions, it appears that especially in developed countries there is a potential desire to contribute to the process, but there is no clear outcome.

There is an increased need for successful collaboration of CSIRTs to be highlighted. Many case studies, including those featured in this document, show that there are unique but valuable approaches that are worthy of further discussion and dissemination. One example is the OECD report, detailing CSIRTs and appropriate metrics, to which all IGF BPF lead experts contributed. This type of report is widely studied and read, and is a great way of organically introducing the CSIRTs' needs to the wider policy community. By adding insights, knowledge and input to policy circles, mutual trust can be built, and mutual understanding achieved.

From a clash of cultures to a mash of cultures? The OAS reported that to acknowledge the work of CSIRTs within meetings and work is common practice for the organization. They even bring the different communities together actively to develop this type of collaboration.

For commercial CSIRTs an additional hurdle may be in place. Any form of cooperation, let alone the exchange of data, may attract the interest of competition authorities[34]. Security is a topic that could be part of competition -one vendor may claim to be most secure in the market- but could also be looked at as a neutral topic, which allows for more effective information sharing. If all have the same problem, how can they solve it for themselves, but also for the common interest? While most commercial CSIRTs have partnered successfully within transparent organizations, deep partnerships may require review with relevant competition authorities. This is a topic for future work in which case studies around successful security partnerships that lead to mutual and (perhaps) national benefit can be developed.

[34] This came forward in a virtual meeting in the BPF on "The regulation and mitigation of unsolicited communication" and most likely is of importance here also. It was not pursued in their draft report though, as it was deemed off topic.

While directly developing policy is an unlikely activity for a CSIRT, it is of importance that CSIRTs provide at least some contribution to policy, even if it is simply educating policymakers on their work. Having influence is a two way street. Because the growth of the Internet and the upcoming ever higher level of interconnection some things may never be the same again. Not being present, is the equivalent of not being heard. It is all about evolving to the next level, but also about keeping the good things. A major finding of this Forum is that CSIRTs can have influence through participation in policy processes and it recommends that this participation is continued at both the national and international level. During recent discussions within the FIRST Education framework, it was widely affirmed that CSIRTs should develop the capabilities to work on participation and development of policy and incident response governance.

CSIRTs and privacy

In this Forum there is consensus that CSIRTs are custodians of data protection. This is recognized by Privacy Commissioners and the European Commission. A provision for the work of CSIRTs is part of the upcoming Privacy Directive of the European Union. One of the participants of the Forum, Andrew Cormack, had previously published a paper with guidelines on the implications of privacy on incident response. He notes that in the context of European law, there are four major elements to be considered in the exchange of information:

- Is Use/Disclosure necessary?;
- Does the action support legitimate interests?;
- Are the data subject's interests protected?;
- Is processing justified?

While the full paper provides more detail on how to perform these tests, there is likely to be significant value for the CSIRT community to exchange their experiences in meeting legal requirements. Possible ways forward lay in the community exchanging these experiences, participating in multi-stakeholder dialogue that ensures that privacy, or better data protection, and sharing both internal and community CSIRT protocols.

- CSIRTs

How to conduct incident response activities in privacy-protecting ways? Guidelines could be developed, as well as tools, e.g. traffic light protocol, or perhaps a lightweight privacy impact assessment, if a more formal approach is wished for.

How can a CSIRT demonstrate that it protects data/privacy? What could be looked into is what level of transparency can be provided on what information you share with whom in what circumstances.

- Policymakers (and other concerned parties involved)

The question from a CSIRT perspective is, how to communicate that incidents can harm privacy

and how incident response can reduce/eliminate that harm. Here a role for policymakers is foreseen. They have to ensure that a country's national CSIRT is trusted to protect privacy.

More in general it was added whether CSIRTs ought to receive a role as the "good custodian" of lost, stolen or leaked (privacy sensitive) information, so non-public data on the Internet. If guidelines were to be developed on how to deal with this sort of information and how to send it (as close) to the source as possible, immediate problems are resolved and transparency reached. At the same time this could be a part of the solution that ethical hackers are looking for as discussed on responsible disclosure below.

Track records in assistance

A dissenting opinion on the questions put to the Forum stated that it is not important whether something is called a CSIRT or not. It ought to be about the track record in providing assistance. In this vain it is important to note that a few respondents name commercial CSIRTs as the most successful, in a general way. As voiced by Team Cymru: "*Real operational issues are managed still by closed groups based on vetting on individuals, and no "approval" from any state will change that in the near term*[35]". The debate ought to focus on successful organizations and not-successful organizations, when asked for assistance. From there a study is possible that brings the gap to light. In short, it is contested that some organizations are not CSIRTs but call themselves CSIRTs and others that do not call themselves CSIRTs may be successful partners.

A suggestion put to the Forum was whether ISPs with notorious reputations, where non-cooperation towards cleaning up of customers or data is concerned, should be blocked from the Internet. This was answered that experience shows that there are many reasons for non-response, that are far from the intent of evil. E.g. language barriers, understaffing, etc. That leaves perhaps a certain percentage. This could be an area for future work.

Responsible disclosure

Another unresolved issue is the position of ethical hackers. The topic was a parallel session[36] at the GCCS 2015[37] and is one of initiatives of the Global Forum on Cyber Expertise that was launched during the GCCS 2015[38]. The session at the GCCS had not only hackers as a driving force, but also the (then) Dutch Officier van Justitie (District Attorney) Cybercrime Lodewijk van Zwieten and representatives of large corporations. At the closure of the GCCS those interested started the Working group for Organizing Coordinated Disclosures. The contribution of this working group can be found in annex 4.The topic of responsible disclosure was taken

[35] Who, What, Where and How. An Insider's View to Participating in the Security Community. Presentation by John Kristoff of Team Cymru at FIRST (2012). http://www.cymru.com/jtk/talks/first2012-community.pdf

[36] Find the session description here: https://www.gccs2015.com/programme?programme=2 You can view the video here: https://www.youtube.com/watch?v=INpAGZUr5TE&t=9685

[37] https://www.gccs2015.com

[38] https://www.gccs2015.com/gfce

seriously by the participants of this Forum. The following contribution shows that the subject has been taken on by the CSIRT community.

FIRST SIG

In 2015, FIRST, the Forum for Incident Response and Security Teams, initiated a Special Interest Group (SIG)[39] for its members on vulnerability coordination. The SIG was proposed by ICASI, the Industry Consortium for Advancement of Security on the Internet, an association of several technology companies, but includes participation from across the CSIRT community.

The SIG maintains the following goals:

- Develop and execute a strategy for improving vulnerability coordination globally;
- Develop and Publish a common set of 'coordination principles';
- Develop and Publish vulnerability coordination best practices which include use cases or examples that describe scenario and disclosure paths;
- Collate and Publish a compendium of coordination resource documents;
- Review and Recommend methods for reporting/updating coordination directories (finding a contact (maybe a directory - a trusted contact).

While less focused on researcher coordination than both other groups, the SIG aims to address the issue of coordinating complex security vulnerabilities that have many affected parties -events such as the Shellshock a.k.a. Bashdoor or Heartbleed vulnerabilities.

The topic could be of interest to this Forum, because a better relationship of ethical hackers versus industry, CSIRTs and the law can have a positive effect on the volume of security breaches. Mark Goodman in his book 'Future crimes'[40] even propagates "contests" between thousands of interested individuals to search for vulnerabilities in software, what he calls "Gaming the system" [41].

The online discussion in this Forum points to the need of establishing guides for prosecutors and/or Memoranda of Understanding that allow ethical hackers to work in a way that "*prosecution is not in the public's interest*". As such it is one of the initiatives in the Global Forum of Cyber Expertise. The government of The Netherlands is said to make responsible disclosure a topic during its presidency of the European Union in the first half of 2016.

If anything, these working groups indicate that the role of CSIRTs is likely to grow where coordinating security vulnerabilities and the way they are addressed is concerned. This indicates some level of awareness should be built into CSIRTs. It also implies there is a close correlation with the trust a CSIRT has. If a CSIRT is run by a law enforcement or intelligence function, will

[39] FIRST Special Interest Group on vulnerability coordination
[40] Future crimes. Mark Goodman (2015)
[41] Ibidem, p 383-385

it have the reasonable ability to assist security researchers, whose work is beneficial, but may in some cases take place around the edges of existing laws?

This Forum recognizes the importance of the topic of responsible disclosure, invites further research and recommends interaction between the FIRST SIG, the OCD Working group which came out of the GCCS, and the GFCE initiative.

- Insights gained as a result of the experience

There is consensus that funding is one of the basic elements for success for CSIRTs. It gives it a chance to employ knowledgeable people, set targets, travel and interact with colleague CSIRTs. It is however no guarantee for successful cooperation and building trust. The chance to reach this level is provided for at best.

There is a tendency towards consensus that participation in and intervention at policymaking procedures allow CSIRTs to be heard and have influence.

The role of CSIRTs seems to be changing in the face of interests professed by many other stakeholders in the work of CSIRTs and the importance given to the work of CSIRTs. This Forum has provided some successful examples of this expanding role and new ways of cooperation. At the same time there is a clearly expressed concern that these new roles, when not understood or applied in a right way, will lead to the loss of trust and cooperation.

- CSIRTs in Developing and Emerging Economies

One participant specifically noted an interest in understanding better how CSIRTs are being developed in developing and emerging economies. From a contribution from Africa it is made clear that in many African nations CSIRTs are non-existent or not mature. The challenges faced are at a basic level. Knowledge, awareness, education, funding, trust, all need to be improved. There are a few successful CSIRT examples in Africa, but in general there is a need to bring the right people to the table, with the much needed knowledge and experience. A second issue brought forward was that where there is a CSIRT in Africa, often issues around the trust to share data arise, in particular because of the common enforcement role assigned to these CSIRTs.

- Proposed steps for further multistakeholder dialogue

In this section the outcomes and recommendations of this year's process are presented. This Forum strives for a translation of the outcomes of this work into actions at different levels by the respective stakeholders, either together or individually and sees a role for the MAG here.

There were several breakthrough findings that have made the work of the 2015 Forum valuable to the CSIRT community and beyond. If this year's process showed something it was the ability of the CSIRT community to face the most challenging questions and comments, some that go to

the core of its mission and rationale, and to come up with answers and (the start of) adaptions to a newer reality.

Several challenging topics lie ahead, e.g. security incidents in the cloud, CSIRT maturity, CSIRT metrics, cooperation with LEAs, etc.. CSIRTs' work is evolving which involves changes to common, well tested approaches. It is because of these two reasons that the Forum recommends that the work is continued in 2016. Both as a driving force for the CSIRT community itself as well as a reach out mechanism to other stakeholder communities.

Work could continue as a Best Practices Forum, which is actively supported by several experts. However, a Dynamic Coalition could also be considered, and would have the benefit of being able to expand the scope from CSIRT to Cyber Security in a broader sense. The lead experts believe there is value in this widening of scope, and bringing the wider security question to a multistakeholder group of participants.

The role of CSIRTs is expanding due to outside forces from governments who require higher levels of national and economic security. The Forum acknowledged these changes and invites further debate so that the main qualities of CSIRTs are kept, while adoptions are discussed, leading to informed changes. An important question to be raised within the CSIRT community, is whether the definition of a CSIRT still qualifies in 2015 or is a change to newer realities required?

CSIRTs have found out that active participation in policy processes, leads to direct influence. Their key messages are heard, better understood by policymakers and become part of the decision-making process.

Responsible disclosure of information in the possession of ethical hackers is a topic that needs further debate among stakeholders. The Forum recommends further study into the topic and interaction between the relevant stakeholders. It is of the opinion that the debate around responsible disclosure would benefit from further discussions in a multistakeholder setting such as the IGF and should be considered for a new BPF in 2016.

Recommendations

Recommendation 1: There is a need for policymakers to discuss the role of CSIRTs with the CSIRT community to avoid misconceptions around the role of CSIRTs.

Recommendation 2: CSIRTs are recommended to be actively involved in relevant policy discussion at both the national and international level. In order to engage with other stakeholders it is important to be where they are. The provided examples show that it brings influence and understanding.

Recommendation 3: Every government has the right to create the CSIRT it needs. It is recommended though that governments make an informed decision, taking into consideration the potential consequences of their choice.

Recommendation 4: Where CSIRTs are concerned privacy and security have to stand together in order for a CSIRT to be truly successful.

Recommendation 5: Data protection is a term that is better understood in a general sense than privacy. Hence it is advised to use this term in a CSIRT context more as it is far more concrete.

Recommendation 6: Data protection has to be at the core of the work of a CSIRT.

Recommendation 7: It is recommended to involve Data Protection Commissioners more in the work of CSIRTs.

Recommendation 8: To ensure transparency and accountability where data protection is concerned, it is advised to make a study whether a standard protocol can assist attaining transparency, as well as more conscious decisions about limits to data sharing, anonymization of data where possible and the handling of data by CSIRTs.

Recommendation 9: CSIRTs should minimize data collection and processing, while also focusing on their constituency and anonymizing relevant information.

Recommendation 10: A well-run CSIRT is an essential part in the protection of data and security within a society.

Recommendation 11: Further study is recommended into the expanding role of CSIRTs. This could e.g. include whether there are sensible limits to tasks given and what role a CSIRT can play in enhancing cooperation in the security chain between other stakeholders, e.g. manufacturers of ICT products and providers of ICT services and does the current definition of a CSIRT match the reality of work asked and tasked.

Recommendation 12: Further study is recommended into the ways CSIRTs and law enforcement can enhance their cooperation in meaningful ways, each from within its respective mission.

Recommendation 13: Further study is recommended into responsible disclosure and how to create conditions that ethical hackers can contribute to a safer Internet experience for all.

Recommendation 14: CSIRTs have a role in handling effects of cybercrimes and providing technical support for investigations, but cybercrime is overall crime and as such should be dealt by law enforcement entities, like the police. Containing too much of this work within a CSIRT, or making a CSIRT part of a law enforcement agency is likely to have significant impact on its ability to work with the private sector.

Recommendation 15: The work of this BPF is seen as extremely valuable by the community. It is recommended to be continued.

Annex 1. Recommendations of the 2014 BPF process

"1. 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 fellow CSIRT. Cooperation and the development of CSIRT in different parts of government is an area that needs further development and discussion.

2. 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.

3. 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.

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

5. The implementation of good standards. There is a need for swifter implementation of Internet standards and good practices in general, and for an understanding of how CSIRT can contribute to this.

6. Cooperation with Law Enforcement and other regulatory Agencies. Mandatory cooperation with Law Enforcement Agencies (LEAs) tends to lead to reduced trust between CSIRT. On the other hand, some voluntary cooperation can often be helpful to certain types of investigations and reduce the overall issue of cybercrime. This thin line would benefit from further discussion with other stakeholders involved.

7. Training, education and participation in international meetings. The importance of this topics cannot be stressed enough in ensuring the success of a CSIRT. Capacity building in the CSIRT community requires further development.

8. The development of case studies. There is a need for extensive case studies, like e.g. happened with DNSChanger and Conficker, in the light of (the implementation of) lessons learned, potential cooperation with other stakeholders and reporting mechanisms in different jurisdictions".

Annex 2 Case study of Switch-CERT by Serge Droz.

"*Cybercrime is money driven. Thus, making cybercrime more expensive is, besides arresting criminals, one way of reducing cybercrime.*

CERTs can't do this on their own any more. Today the value chain in the Internet is quite broad with several service providers, such as registrars, hosters, web designers etc. Criminals need infrastructure too. But hey typically prefer taking over buying. Today a lot of criminal infrastructure runs on compromised hardware, be this hacked home PCs or hacked (web) servers.

SWITCH-CERT has two programs to tackle this issue. Initiated by Team Cymru's Cert Assistance Program SWITCH CERT today processes thousands of IPs from hacked PCs daily. Different sources are aggregated and then distributed to respective network owners for remediation. Since last year these efforts are supported by the Swiss Internet Security Alliance. It's members, Banks, ISPs and hosters coordinate the effort of cleaning infected PCs by providing a common help to end users and sharing intelligence.

Operating the registry for the ccTLDs .ch and .li SWITCH closely works with the regulator to create a legal basis to fight the misuse of domain names. The registry now has the power to shut down a domain name if it is used to steal personal information (phishing) or distribute malware.

SWITCH today has a comprehensive program, working together with hosters and registrars to solve these issues before blocking. This means that over 80% of all incidents are cleaned up in less than a day.

The close collaboration with all involved stakeholders was crucial to the success. We regularly meet with them and discuss how collaboration could be improved. We inform and provide tools to fix the issues.

A recent, external study, analysing all publicly available information (Blacklists etc) concluded that .ch is the safest open ccTLD.

Misconception: CERTs should create Awareness. It's important but it's not clear how efficient it is. Fact: CERTs must work closely and protectively with all stakeholders to be successful."

Annex 3. Case Study by KrCERT/CC

"*Korean government such as the ministry of science, ICT and future planning with Korea Internet & Security Agency, a mother organization of KrCERT/CC, conducts many reactive and proactive services to rapid respond to incidents and prevent spreading damages. The DDoS Shelter Service*[42] *and the Cyber Curing Service*[43] *are the representative of the government-led reactive services in South Korea.*

The DDoS Shelter Service has been operated since 2010 to minimize the damage caused by DDoS attacks on businesses that are not fully prepared. There are a lot of small medium-size enterprises such as online shopping malls in Korea due to advances in the Internet service. Also, it is a fact that some of them haven't been fully equipped to respond to security incidents by themselves. Therefore, the Korean government provides the DDoS Shelter Service for small and medium-size enterprises which cannot respond to DDoS attack in order to not only minimize economic damages of victims and protect their assets but also their customers continuous use the web services without disconnection. However, the DDoS Shelter Service isn't for anyone. Compromised enterprises cannot use this service continuously if they have the same attack after they got DDoS attack before. Enterprises, if they have the capability to equip or if they always become a target of DDoS attack, should protect their customers by their own countermeasures. The government encourages small medium-size enterprises in improving security awareness and capacity until they are ready to protect their assets, customers.

The Cyber Curing Service aims to directly remove malwares from compromised PCs and it has been operated since 2011 after outbreak of a nation-wide scale of Internet incident in South Korea. This service is a web browser based notification service with one-time dedicated anti-virus software which targets only one particular malware type. The Korean government developed notification system which cover most of Korean Internet service subscribers with Korean Internet Service Providers. One vendor can protect its customers only, however, if the government and the enterprises cooperate closely, we can protect most of Korean citizen.

The reason we provide the government-led reactive services is that we are responsible for protecting Korean people. We strive to let Korean users use the Internet service without cyber threats and for enterprises, we guide them so they should protect their customers and themselves through raising security awareness."

[42] http://eng.krcert.or.kr/service/ddos.jsp
[43] http://eng.krcert.or.kr/service/cyber.jsp

Annex 4. Working group for Organizing Coordinated Disclosures (OCD) by Inbar Raz

This informal Working group has as members the hacker community, large corporations, a district attorney, policymakers, representatives of CSIRTs and others. The purpose of the Working group is to find a way to allow researchers to do their work, without fear of prosecution or persecution, while at the same time protecting the vendors from unnecessary actions, exposure and/or damage. The key word here is Ethics.

The Working group aims at a Government-sanctioned Code-of-Conduct. A document that says: "If you did everything according to the rules in this document, then you will be protected from criminal prosecution". That would be the ideal outcome of the OCD. If needed it can be accompanied by a law or just by a formal directive for prosecutors. The people in the working group see responsible disclosure as reporting function, like e.g. on corruption. This Forum received a national example of a country where this process is well underway between stakeholders.

Israeli pilot on disclosure

Currently there is a pilot running in Israel. Security researchers, the hacker community, police and Government were brought together. A process was started with the intention to create a government-sanctioned procedure, that will allow for responsible research of security vulnerabilities, as well as a coordinated disclosure process, which aims to guard the interests of all involved parties (General Public, Vendors, and Researchers). It's intended to finish the work in Israel in a relatively short term, and then present it as an example for other countries, as well as for the efforts in the OCD Workgroup.

There are several questions being addressed by these and other working groups which are relevant to the function of the CSIRT community.

1. What is a "proper way" to conduct research on someone else's vulnerabilities?

- *How can one perform the research without causing damage to existing data and services?*
- *How can one perform the research without breaching an unnecessary level of privacy?'*

2. What is the "proper way" to report the vulnerability to the vendor?

- *How long after the research has been completed, must one report?*
- *What content must be minimally included in such a report?*

3. What is the best way to publish your research results?

- *Are there any timing constraints?*
- *Can the vendor impose a time frame? If so, who regulates that time frame?*

Should it be required to supply the vendor response?