IGF Best Practices Forum on "Establishing and Supporting CERTS for Internet security

Report 6. Incident management

Note. This report joins the comments on the online forum. As there were distinctive topics that were discussed, they are presented separately. Entries are presented in the order of arrival. First the contributor is mentioned and where appropriate within brackets the person responding to is mentioned, e.g. (Wout). The affiliation of a respondent is not mentioned, as he/she may be giving a personal point of view or not. As consultant to the group this is impossible and not necessary to ascertain.

Olawale Bakare (on Rohanna in report 1 general discussion)
Let me make add this to the ongoing discussion.

The CERT practice discussion should vary and, evaluate the existing practices either at regions or nations.

And i think, it is highly important to focus management strategies that are in existence and currently being adopted by them, in particular on:
1. incidents occurrence
2. how do such systems work around problems? However, the objectives of problem management should address:
   a. the amount of reccuring incidents, do the systems eliminate them?
   b. incidents impossible to resolve?
   c. what level of impact of incidents that look so unavoidable?

Adli Wahid

I think most people would probably agree that have an incident response
>team or capabilities is critical these days for most organisations (or
>countries for that matter). Some organisations require it as part of the
>Enterprise-wide risk management framework or cyber security strategy.
>
>There are some good available resources out there of how to go about
>setting up & running a CERT/CSIRT. One very good example is available
>from ENISA¹s website here:
>
>https://www.enisa.europa.eu/activities/cert
>
>And I think a few other organisations have developed similar guides so
>that it is easy to understand how the organisation can be structured, what
>tools are needed to run the operation and so on. If you know of any other
>sources of reference like the above please let us know.
>
>Establishing a CERT/CSIRT is one thing - running it successfully is

>probably another story. For this Best Practice initiative we are also
>interested in learning the challenges that are faced by CERT/CSIRTs. I
>think Patrick already mentioned that not having clear definition of the
>role can lead to operational problems (lack of trust). Funding is probably
>another one - without which teams are not able to for example acquire
>tools or hire staff (or send them to conferences / training).
>
>Please share your observation on some of other challenges or issues that
>could affect the operation of a CERT/CSIRT. Thanks!

Andrew Cormack (on Adli)

One of the biggest barriers I hear about (maybe because of my job title nowadays) is that CERTs think the law prevents them doing incident response. In fact I'm usually pleasantly surprised when I actually talk to regulators how much they do 'get' incident response - "incident response protects privacy, of course we support it" was one comment from a national privacy regulator. So maybe we should be engaging more with regulators to ensure that legislation does leave us the space we need and that we agree on how to use it?

One area that does concern me is where countries are creating special laws for their national CERTs. I think there's a risk there of creating undesirable barriers between those CERTs and the others in their countries. If I'm an 'ordinary' CERT and my constituents share information with me knowing that it's protected by 'ordinary' law, will I lose my constituents' trust if I share it with a national team that has special exemptions from that law? That concern has also been expressed when dealing with law enforcement - if I share information with them as intelligence, do I lose control of whether it may eventually turn up being used as evidence in a public court? So I think it's important for teams that do have special powers or authorities to also offer agreements on how shared information will and won't be used. Otherwise there's a risk that less information will go to them than Internet safety requires.

Adli Wahid

I mentioned in my previous email about resources or references available out there on planning, creating, managing CERTs/CSIRTs.

1. Incident Management Publications - http://cert.org/incident-management/publications/index.cfm

2. ENISA repository on CERT/CSIRT - https://www.enisa.europa.eu/activities/cert

Do you know if there is anything else out there? perhaps in different languages that could be added to the list.

Keisuke Amata

This is Keisuke Kamata,

I'd just share some list in my mind.

A. JPCERT/CC publish Japanese version of CSIRT documents.
http://www.jpcert.or.jp/csirt_material/

B. Not sure about this but NIST SP800-61Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

C. RFC2350: Expectations for Computer Security Incident Response
http://www.ietf.org/rfc/rfc2350.txt

Maarten van Horenbeeck

These are two more documents which are not necessarily guidance on how to start a CSIRT, but help assess its capability/maturity:

FIRST Site Visit Requirements:
http://www.first.org/membership/site-visit-V1.0.pdf
http://www.first.org/membership/site-visit-v2.0.pdf

Trusted Introducer Security Incident Management Maturity Model:
https://www.trusted-introducer.org/SIM3-mkXV-TI.pdf

They are used to help assess whether a CSIRT meets the requirements to be a member of FIRST, or to independently gauge the maturity of a CSIRT for certification in Trusted Introducer respectively.

In 2009, GovCert.nl (now NCSC-NL) of the Netherlands also published "Cert-in-a-Box" with lessons from setting up GovCert.nl:

http://www.first.org/resources/guides#bp21

One of the older documents on establishing a CSIRT comes from AusCERT in Australia. This dates back to 1995 but still retains some interesting notes and personal experience:

http://www.auscert.org.au/render.html?it=2252

Markus Kummer

Just a reminder: if not already done, please also send links to relevant documentation to the dedicated email address at the IGF Secretariat:

discussion_questions at intgovforum.org

This will allow the Secretariat to create a publicly available repository of background information on the IGF website.

Miroslav Maj

It is just worth to add that many ENISA publications are available in
various languages.

For example " A step-by-step approach on how to setup a CSIRT"
(https://www.enisa.europa.eu/activities/cert/support/guide) is available
in 26 languages including Chinese or Hindi.

Robin Ruefle

I have some additional materials/resources to add to the list. Unfortunately only in English. :-) These are some of the documents in the link that Adli mentioned below in the Incident Management link.

>*From CERT at the Software Engineering Institute, Carnegie Mellon University*

CSIRT Frequently Asked Questions
http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm
a short list that provides quick answers to some common questions about CSIRTs

Creating a Computer Security Incident Response Team: A Process for Getting Started
http://www.cert.org/incident-management/products-services/creating-a-csirt.cfm
a brief white paper describing some of the basic requirements for people to consider when creating a CSIRT capability

Action List for Developing a Computer Security Incident Response Team (CSIRT)
http://www.cert.org/incident-management/csirt-development/action-list.cfm
a high-level overview of the actions to take and topics to address when planning and implementing a CSIRT

CSIRT Services
http://www.cert.org/incident-management/services.cfm
a descriptive list of the typical services that a CSIRT might provide (this is extracted from content that also appears in some of the above documents, it has just been separated into a separate document for convenience)

Staffing Your Computer Security Incident Response Team - What Basic Skills Are Needed?
http://www.cert.org/incident-management/csirt-development/csirt-staffing.cfm
a short paper describing some of the types of core knowledge, skills, and abilities that successful CSIRTs seek in staffing their team

Handbook for CSIRTs
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305
the original seminal work on creating a CSIRT; based on the experiences of the CERT/CC and other response teams during the early development days. This 2nd edition with updated information was released in 2003

Defining Incident Management Processes for CSIRTs: A Work in Progress
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7153
This technical report delves into the day-to-day work that teams perform, focusing on a process-oriented approach to defining the CSIRT work.

Incident Management Capability Metrics (IMCM)
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8379
adapted from work the SEI did with the DoD and US-CERT, a set of metrics that can be used to evaluate and improve an organization's capability for managing computer network defense.

Mission Risk Diagnostic for Incident Management Capabilities
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=91452
a tool that can be used to provide a quick evaluation of the potential for success of an organization's CSIRT or incident management capability (IMC). It can be used as an independent technique, or in conjunction with the IMCM.

Organizational Models for Computer Security Incident Response Teams
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6295
a technical report that expands on information provided in the original Handbook. It focuses on describing different types of teams (a coordinating center, a security team, distributed teams, etc.). It discusses some of the typical strengths and weaknesses for each type.

Incident Management topics on the Build Security In (BSI) website
<https://buildsecurityin.us-cert.gov/articles/best-practices/incident-management/incident-management>The Incident Management section of the BSI website contains articles that provide an introduction to computer security incident management.
Defining Computer Security Incident Response Teams<https://buildsecurityin.us-cert.gov/articles/best-practices/incident-management/defining-computer-security-incident-management-teams>
This paper introduces and defines various aspects of CSIRTS including activities, roles, staff, and mission.
Avoiding the Trial-by-Fire Approach to Security Incidents<http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymattersmar99.cfm>
This report assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.

Case Studies of CSIRTs that were created:
* Colombia<http://www.cert.org/incident-management/publications/case-studies/colombia.cfm>
* Tunisia<http://www.cert.org/incident-management/publications/case-studies/tunisia.cfm>
* Financial Institution<http://www.cert.org/incident-management/publications/case-studies/afi-case-study.cfm>

Materials for National CSIRTs
* Steps for Creating National CSIRTs<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53062>
* Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability (Version 2.0)<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=9999>
* Establishing a National CSIRT<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34434> (podcast)
* Tackling Security at the National Level: A Resource for Leaders<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34478> (podcast)

Although this is an old document - some of the history and best practices are still relevant.

State of the Practice of Computer Security Incident Response Teams

<http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6571>
Many of our documents are due to be updated.

We also offer the following courses:

* Overview of Creating and Managing a CSIRT
  http://www.sei.cmu.edu/training/P68.cfm
* Creating a CSIRT (1-day)
http://www.sei.cmu.edu/training/P25.cfm
* Managing CSIRTs (3-day)
http://www.sei.cmu.edu/training/P28.cfm
* Fundamentals of Incident Handling (5-day)
http://www.sei.cmu.edu/training/P26.cfm
* Advanced Incident Handling (5-day)
http://www.sei.cmu.edu/training/P23B.cfm
* Advanced Forensic Response and Analysis
http://www.sei.cmu.edu/training/P103.cfm

I forgot to include another best practice guide for standing up a CSIRT. It is located at

http://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf

It was a guide done to help the ministries within the New Zealand government stand up their CSIRTs, based on a mandate within the government.

Thomas Millar

There is also the NIST guide on computer security incident handling:

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Jerome Athias

in case of interest, a new book called "Computer Incident Response and

Forensics Team Management"

http://www.net-security.org/review.php?id=327

ISBN: 159749996X

Tarik el Yassem on (CERT/CSIRT toolbox)

Great discussions so far, I'd like to hear your thoughts and experiences with regards to the specific tools we need to be effective as a CERT/CSIRT.

I have found that tools are essential in order to be effective and make a difference. However, in many organisations the CERT/CSIRT is just a tiny group of people with not that much influence and usually viewed as an odd bunch that wants to do things differently.

What I have seen in quite some places is that the CERT/CSIRT spends a lot of effort in the struggle to get even the most basic tools running because the IT department is not supporting it, or 'already have a (helpdesk) ticketing system'. But CERT/CSIRTs need to use more specific tools such as OTRS or RTIR or other tools that need to integrate with a production environment. Much of the tools we need are not suited for enterprise environements, and making the case for IT to allow the use of them is hard once things are not packaged, maintained, documented etc.

When people are establishing the CERT/CSIRT they often think that tools are something that are details to be decided on once a CERT/CSIRT has been established. I think it would be helpful for a CERT/CSIRT to adress this issue during the creation of it.

What are your experiences with this and do you have any thoughts how we could improve on that as a community?

Patrik Fältström (on Tarik)

Interesting question ... I have now set up 3 CERT/CSIRTs (within institutions) and have had differing success with the use of tools and approaches. I revised the technique that I use each time and follow a process, which includes;

Decide on the initial services the CERT will provide, based on page 25 of this handbook;

http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

This decision will be down to various factors, such as the size and make-up of the constituency, the size of the proposed CERT and other factors.

Once I have that, I can then look at the tools that are needed, and build up a requirements list. Generally, these fall into two camps;

Tools for business - these are non-negotiable, they are the very core of the work of the team, and they require certain software and hardware. In this category will be monitoring software (flow, IDS, IPS etc), forensic software, and scanning systems.

Tools for management - these are the ones like ticketing systems. For this, I take a list of requirements that the tools need (eg: confidentiality for investigations) and ask for the existing IT systems to meet those requirements. If they can, that's great! If not, there is good grounds for putting in a system which is non-standard. At this point, the CERT is a customer, and it is for the IT systems to meet the requirements.

Where possible, I will use standard IT supplied systems (it's one less thing that the team has to manage).

Once the systems are in place, it then becomes an issue of building up the processes and procedures that the CERT will work to.

R. Ruefle

This next resource isn't about CSIRTs particularly but incident management in general. But I still think it should be part of the resources we are collecting. This is not an official write-up attached, but provides a summary of the ISO 27035 Incident Security Management - which is in final review right now. I am not sure who wrote this overview.

http://www.iso27001security.com/html/27035.html

The actual copies of the draft standard - are available to those we are part of the review and development processes until it is published.

The older standard is here:

https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en

but only a small portion can be seen for free.

Wout de Natris (on Olawale Bakare)
Following up on your question. Could you elaborate some more on what specifically you are looking for? Also on the reason behind your asking?

For my understanding, is what you're looking for beyond general descriptions that e.g. ENISA, Carnegie Mellon or FIRST provide on their respective websites? I'd like to learn more so that I can elaborate better in the draft I'm writing for this group to preview.

All,

Can anyone else provide other examples out there that could be used as a form of standard manual?

Is there a general believe that standard manuals could help this community further?

If so, where could one be made best?

Olawale Bakare (on WdN)

Following up on your question. Could you elaborate some more on what specifically you are looking for? Also on the reason behind your asking?
I am not really sure i got the understanding of the questions.

For my understanding, is what you're looking for beyond general descriptions that e.g. ENISA, Carnegie Mellon or FIRST provide on their respective websites?

My question was prior to gaining information about ENISA, Carnegie Mellon or FIRST perspectives on CERT/CSIRT.

Andrew Cormack

I suppose one of the things that kicks off the initial interest in a country might be developing a cyber-security strategy? In the UK we've done it the other way around - we had CERTs nearly 20 years before we had a national cyber-security strategy - but others may find top down a better way to get started. If so, ENISA has a collection on those too, including good practice on developing them, a guide book to the most common things they contain, and links off to the growing collection of strategies that already exist. That's at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

I'd imagine that the very first steps for a CERT will depend very much on what event triggers its creation: whether that's a political change or a major incident. As I understand it (it was around 1993, a few years before I got involved) our Janet CSIRT came about because of a major (for those days) incident of university systems getting hacked. As the national network we got involved in helping with that one, and afterwards someone said "maybe we should remember how to do that in case it happens again". So very informal!

Whatever that step 1 is, the community has recognised pretty well that step 2 should benefit from having existing good practice to look at, hence the ENISA and CERT-CC collections that try to provide guidance pretty much whichever angle you are coming from. If you've found a new approach, or just some tweaks that existing approaches needed to fit your particular circumstances, please let us know. Those who come second, third, fourth, can often do a better job than those who went first, because there are all those earlier mistakes there to learn from ;-)

Hope that helps

Wout de Natris (on Olawale Bakare)

Thank you. I was curious to learn if you needed any information beyond what was send later within the group, so I could be as thorough as possible when drafting the starting document. It was answered, thanks.