M&I/Stelvio

Dr. A.P. Jurg
Drs. E.P. Stals
Drs. D.P. Stikvoort

A Trusted CSIRT Introducer in Europe

An empirical approach towards trust inside the European Incident Response scene – the replacement of trust by expectations: used for introducing new teams into the scene and stimulate existing ones to maintain their offerings.

Commissioned by TERENA

Klaus-Peter Kossakowski & Don Stikvoort

M&I/Stelvio
Amersfoort, The Netherlands
info@Stelvio.nl

Version 2.0
February 27, 2000

INDEX OF CONTENTS

1 Aim

TERENA tasked us to describe the process of introduction and accredition of new CSIRTs - in order to bring them into "the web of trust" – and to set criteria (i.e. CSIRT requirements) to foster the objectivity and authenticity of this process.

After a discussion of the current situation and a limitation of the CSIRT scope, we shall come back to this aim and present it in a revised version, to be used further on as deliverable description.

2 Interlude: Definition of CSIRT

To avoid fuzzyness we alas have to bother you here and now with a definition of CSIRT that will hold till the end of this report.

What **is** a CSIRT then?

[RFC 2350] has a good implicit definition:
"Any group calling itself a CSIRT {or CERT or IRT or …} for a specific constituency must therefore react to reported security incidents [1], and to threats to "their" constituency [2] in ways which the specific community agrees to be in its general interest."

However, "react to {…} incidents" is pretty open, so we need [West et al. 1998] to narrow that down:
"{CSIRT:} A team that provides a basic set of services (contact point for reports, support when incidents occur and feedback in regard to requests addressed to the team). Announcement services might also be offered as well as other services as defined by the team. The team might serve different constituencies, and might even provide different service packages or service levels."

The combination of both statements gives a good enough picture of what we conceive a CSIRT to be. Most probably e.g. all the ex-EuroCERT customers entertain CSIRTs – even if they do not use such a label explicitly, then:

If an entity A entertains a FUNCTION B where customers/constituencies can report computer/network security incidents, and B then handles these reports in a constructive way (consultancy, coordination, feedback, …), then function B essentially is the CSIRT of entity A.

The above definition of a CSIRT does not prescribe coordination with other CSIRTs as a necessary task. A CSIRT could in theory be an island, but clearly for the goal of this report such teams are not of interest. In fact such teams deny their constituency potential benefits arising from information exchange, expertise of other teams and supportive information from sites external to the constituency but involved in an incident. Thus:

Interaction between teams on specific incidents, i.e. the task of incident coordination, is an explicit part of the CSIRT definition in this report.

---

1 Incident [West et al. 1998]: any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of such events are:
- Intrusion of computer systems via the network (often referred to as "hacking")
- Occurences of system anomalies like computer viruses
- Probes for vulnerabilities via network connections to a range of computer systems (often referred to as "scans")

2 Constituency [West et al. 1998]: a specific group of people and / or organizations that have access to specific services offered by a CSIRT

3 Situation Report

Organisations slowly build up an incident response capability. The following phases can be separated:

I. Non-recognition: the problem is not recognized, all handling of security problems is done within the line organisations, no coordination to the outside other than per chance. Most organisations inside Europe still are in this phase, and even many ISPs. The US is a few years ahead of Europe: the awareness of the problem is becoming widespread in organisations of medium and bigger size.

II. De-facto incident management: the problem is recognized, maybe an instance to report to is installed internally, but no structural effort inside, nor stuctural links to the outside. In the coming few years the majority of medium sized and bigger organisations inside Europe will grow into this phase.

III. Structured incident management: an incident response capability – let's name it a CSIRT – is available, and is linked to other CSIRTs in the world. Typically these teams are (striving to become) FIRST members, or associated with or customer of a FIRST member. Phase III could be separated into two subphases:
   a. Not yet part of the web-of-trust
   b. Part of the web-of-trust

The approximately 90 teams worldwide that are members of FIRST are mainly in phase III, several tens of them in IIIb : FIRST membership alone is not enough to become part of the web-of-trust, though it helps significantly – but also active participation in the community is needed, say: visibility. One other factor is important also: continuity. If a team cannot uphold its quality (by, for example, distribute wrong information), trust can evaporate.

What then is this elusive web-of-trust that pops up in this report? A definition by example is the best clarification. A team is inside the web-of-trust if it is able to report an incident to another team also inside that web-of-trust and to be taken seriously at once, trusted that the information provided is correct, and be helped with some priority (over average reports). Information from teams inside the web-of-trust are more strongly considered as other information, as the other teams trust the team to know the background of incident response, make realistic assumptions and assessment due to their knowledge [3].

TERENA members will typically be in phases II-III . Especially those in phases II and IIIa – the majority we presume - are of course of interest to this report, since for those there is work to be done: the gradual transformation to phase IIIb.

A breakdown of current FIRST members within Europe shows 27 teams, one third of them affiliated with TERENA due to their constituency and/or parent organization:

- 4 Government teams (1 France, 1 Germany, 2 UK)
- 10 Commercial organizations (1 Danmark, 1 France, 3 Germany, 1 Netherlands, 2 Switzerland, 2 UK)

[3] In the early nineties to become part of the web-of-trust it was essential to go e.g. to a FIRST conference and „drink beer in a pub with the right people" – however useful and enjoyable this still may be, it is not enough anymore, the CSIRT society has become too big, people change places too often, and the financial stakes involved in network security have become too high

- 4 "other" teams (1 Germany, 1 Israel, 1 Italy, 1 UK)
- 9 research and educational networks (1 Danmark, 1 Germany, 1 Kroatia, 1 Netherlands, 1 Poland, 1 Scandinavia, 1 Switzerland, 2 UK)

It goes without saying that the above suggested sequence – growing from phases I and II via IIIa to phase IIIb - is the way to go ahead. This is based on the fact that the current cloud of IIIb teams is doing their work moderately well, and –more importantly- that it is ***impossible*** *to keep on doing this work by just expanding the cloud and covering everybody who sends a mail and says: "he, I'm a CSIRT, trust me, send me mail". Elusive as "trust" may be, the latter approach is clearly a bridge too far. The trusted cloud must not be expanded, but rather new teams should be drawn into the cloud. The big problem clearly is to retain quality with the cloud becoming denser and denser.*

If we broaden the TERENA perspective – what is exactly what we shall do when defining the scope of CSIRTs in the following chapter - to not only look at TERENA members (mainly research ISPs), but also commercial ISPs, major companies and governmental institutions, plus vendor-product teams and major commercial CSIRTs – all inside Europe - then phases I and II will be pre-dominant. The transition of phase I to II is a gradual one that will take place in the coming few years – the situation in the US is ample proof for that assumption. It needs only background help from national and international initiatives and can thus be fostered by organisations like TERENA, FIRST and established CSIRT teams. This however is clearly outside the task set for us by TERENA.

Two important remarks have to be made at this stage. First of all that even being in phase IIIb does not imply that a CSIRT is a fully established entity – the phenomenon is too young for that. "Many CSIRTs in existence today either lack a clear understanding of their goals and objectives or have failed to effectively communicate that information to the parties they interact with" [West et al. 1998]. As a result, they needlessly expend effort and resources (often in crisis situations) in an attempt to

- Understand if they are using the correct priorities to ensure they respond to the most important activity.
- Correct any inappropriate expectations of those they interact with
- Understand how and if it is appropriate for them to react to a given situation.
- Revise their policies and procedures to meet the needs of the situation.
- Determine if the range and nature of the services they offer should be modified.

Until a CSIRT defines, documents, adheres to, and widely distributes a concise and clear mission statement and service definition (as e.g. per [RFC2350]), that situation is unlikely to improve. The consistent lack of time that plagues CSIRTs however does not help the improvement of this situation very much. For the sake of this report we choose to ignore this problem/challenge – we falsely presume here that all that matters is to become part of the web-of-trust. However we shall indirectly contribute to the improvement of this situation by introducing criteria for CSIRTs to meet to help them grow into the web-of-trust: these criteria will be of the useful structural kind (like service definitons) which have been grossly neglected by most old-hand teams because of their pioneering status and lack-of-time[4].

The second important remark is that if we are to define a process which would bring teams from phases II to IIIa and then IIIb, and criteria for teams to meet to help that process along,

[4] Of course several of the old-hand teams have meanwhile corrected the situation and produced service definitions etc.

that also implies that these criteria would be useful to apply to existing IIIb teams. This is far from implying some sort of certification of CSIRTs – time is not ripe for that yet – but it is about an important notion, and that is "trust maintenance". Now this is a rather new idea in this game. The interesting thing is that it takes years for teams to gain trust, and usually this trust is based for 90% on a few key personal relationships which have been built carefully – and only for 10% on written service or quality statements, site visits and so on. What one sees then is that after the trust has been gained, the key people often move to other places – but magically the trust invested in the team remains – based only on the 10% that is left. This is a potentially dangerous situation, and if only a few things go really wrong, the relationship is wrecked for the years to come. Trust takes years to gain but is lost overnight. What would help the situation much is to improve on the 10% part: initially trust is indeed based much upon personal relationships, but once established the structural part (the 10%) should be increased gradually. This again means an emphasis on objective criteria which can be met. And it means that IIIb teams should care about these criteria just as much – probably even more – than IIIa teams, since IIIb teams are much more vulnerable when walking on the waters of trust.

Thus a well defined transfer of phases II to IIIa and IIIb, **and** staying inside the latter phase, the trust-phase, is the topic of this report. It needs saying that gaining entry to the CSIRT community today can be a difficult and lengthy process. The community is ready to embrace new members, but it is wary of interacting with new CSIRTs unless an existing member of the trusted community can vouch for them. So some new teams are in a "Catch-22" situation, wanting to contribute, but needing to gain acceptance and mentoring from an existing member of the community before they can begin to gain broader acceptance. As most teams have no charter or funding to act as mentors to new members of the community, finding a mentor and introducer is not as easy a task as it sounds.

Moreover, because there is no formal mentoring process for new members of the community, the guidance given to new teams can vary widely depending on the experiences and time available from their mentoring team. As a result, the CSIRT community expands at a much slower rate than is needed, and the teams operate with a widely varying set of operations and standards. The community needs to ensure and adopt a sponsorship process that doesn't depend on the good will of individual teams and ensures that each team meets an agreed-upon minimum level of operational standards.

In the words of [Kossakowski et al. 1999]:
„Today's approach is not reliable, does not scale, and it must be made more effective. It is critical to have a global response infrastructure to replace a less reliable system based on trust between individuals with a reliable and effective system based on global understanding/agreement."

FIRST could play a much more active role to help establish and maintain such an infrastructure. However, as long as FIRST is entangled in its change process from an all volunteer effort towards a professional organisation with services funded by its members, it will not be able to assume this role. Any movements in this direction are not expected to start any sooner than in 2001 – this and the uncertainty of it make it impossible to rely on. ISOC and IETF are not expected to fill in this gap on the short run. Therefore especially regional initiatives have a good chance of succeeding. In Europe the research CSIRTs together with TERENA have been in the lead since 1992 and are therefore in an ideal position to achieve inside Europe what FIRST is currently not able to take on. Good

cooperation between TERENA and FIRST would be the best way to avoid precious efforts being spoilt in this area.

This report intends to do just that: define a more or less objective process (built on criteria) for TERENA to implement as a sort of *trusted introducer* to help organisations evolve from phases II to IIIa and IIIb. A process irrespective of FIRST – though indeed the implementation of such a process postulates a relationship to FIRST and could even be seen as the prelude to a conceivable European chapter of FIRST. In fact, the adoption of the process - once it has shown its success - should be suggested to FIRST. It is expected that TERENA can and should play a leading role here for the next 3 years to come – after that probably a process will take place as we witnessed when the RIPE NCC grew up and left the parental TERENA house to stand on its own. The comparison is in many ways interesting. However, it is unlikely that the *trusted introducer* will come to stand on its own: it is expected that it will liaise with FIRST or a FIRST follow-up, or with other suitable umbrellas. It is also not very likely that security will become so trivial that the CSIRT system will become useless, nor is it very likely that law enforcement will “take over”: the international cooperation of law enforcement is a daunting problem compared to CSIRT cooperation, and besides, most organisations shy away from relying on law enforcement for the sheer complexity (and cost) that comes with computer forensics and for the fact that they don’t want to see their names in the newspaper – which is a viable risk when a lawsuit takes place.

4 CSIRT Scope

As hinted on above it is useful to state what CSIRTs – or potential CSIRTs - we shall be referring to in this report.

Following the above CSIRT definition, the potential number of teams is clearly a daunting one. There are a few ways to narrow that down. The first one is geographical limitation. TERENA's geographical constituency is Europe plus neighbouring countries, and this report follows that limitation – though the conclusions of this report would essentially prove valid worldwide as well. Of course incident coordination - and therefore the web of trust - does not stop at the European borders – *It is supposed however in this document that key teams within the European framework do have access "outside", i.e. to key CSIRTs outside Europe* [5] *, for the sake of incident coordination.*

We could narrow the number of CSIRTs further down by following the TERENA constituency more closely, and only consider CSIRTs in the educational or research areas. 5 years or so ago, when those areas more or less **were** the Internet in Europe, that may have been a viable approach – but clearly not anymore– it has become impossible to single out a "research island" inside European networking. Therefore this limitation will not be pursued [6].

There is a more practical way to limit the scope, and that is to state what kind of CSIRTs we are interested in for the sake of this report. That list is surprisingly short:

- ISP teams (both commercial and non-commercial)
- Government related teams (including military and law enforcement)
- Vendor teams (with regards to the security of their products, not their internal security)
- Teams for major international institutions or companies including vendors (served by several ISPs)
- Major commercial service providers that offer incident response and strongly related services (providing an "outsourced" CSIRT for the customers)

Agreed, this is a somewhat arbitrary list, but utterly practical. It leaves out the big numbers of (potential) CSIRTs because it hides all those behind ISPs – leaving the building of a "web of trust" for the ISP customers to the ISP itself. As it should be: an ISP delivers a service, so must take care of the essential security aspects of that service, which must include the ability to "handle complaints" (i.e. handle incident reports).

To conclude: the CSIRT scope of this report is limited to (potential) CSIRTs within TERENA members (mainly research ISPs), commercial ISPs, major companies and governmental institutions, plus vendor-product teams and major commercial CSIRTs – all inside "bigger" Europe. As remarked in the preceding chapter we shall concentrate on organisations in phases II or higher – those that realize that they have to actively deal with security incidents

5 Like CERT/CC, CIAC, AUSCERT etc.
6 Neither was it by TERENA: note e.g. that EuroCERT's services were not limited to the primary TERENA constituency

– canvassing organisations that are clueless in this respect is outside the scope of this report.

5 Revised Aim

The original aim as stated above was:
“to describe the process of introduction and accredition of new CSIRTs - in order to bring them into "the web of trust" – and to set criteria to foster the **objectivity** and authenticity of this process. “

With the work done until now, we *could* revise that aim to include the CSIRT scope limitation and make it more explicit in mentioning that we are interested in the transfer from phase II to IIIa and eventually IIIb, plus the maintenance of that phase. This would be the work for what we called a *trusted introducer*.

However, for a *trusted introduction process* – we prefer the generalized term from now on - to **verifiably** work with the subjective “belonging to the web-of-trust” parameter used to distinguish between CSIRT phases IIIa and IIIb is no good. Neither are the differences between phases I, II and III very useful in this regard, because though they are fairly objective parameters, they are hard to *show* in an **objective** way. The only way a *trusted introduction process* is going to work is taking an essentially empirical approach: collect data, apply templates, establish the authenticity of information and maintain it. That’s *TI* in a nutshell:

*We shall refer to the **trusted introduction process** as **TI** in this report from now on. We shall apply the term in a generalized sense, where TI means both the process itself and/or the party/parties implementing the process.*[7]

So, when you look at it from the perspective of already established CSIRTs, *TI* must ensure the replacement of trust by expectations – expectations that are based on objective statements that are verifiable.

The revised aim hence becomes:

*The aim of this report is to describe **TI** : an objective process meant to be applied to teams within the above defined scope, that will enable teams new to the CSIRT community to move to a **level** where other teams will find it relatively easy to share information with them and work with them on incidents (in other words: to **trust** them) – and that will enable teams (also the already established ones) to **stay on that level**. To ensure the process’s objectivity **TI** will be fully based on objective statements that can be verified – these statements will be worked out in detail, in the form of criteria.*

TI is rather abstract, agreed, which makes reading difficult. To help the reader on that account, we run ahead of things a bit by stating already that it is highly unlikely that everyone, who has a need to rely on another team in e.g. in incident case, will be able to verify the objective statements about the other team individually. *TI* is obviously performed

[7] one might name this generalized use of *TI* rather fuzzy: however this „fuzzyness“ considerably enhances readibility and we are quite confident that the reader is well equipped to immediately grasp the specific intention of any incarnation of *TI* from the context – human logic and fuzzy logic blend rather well

at only few places, by instances that we already named *trusted introducer* in this report. Just think of *TI* as a concentrated function, a whole entity, therefore.

6 Specification of Objective Criteria

To describe *TI* – a process built on the objectivation of pre-set criteria – without first defining the criteria would be an interesting exercise in generalisation indeed but rather a waste of the reader's time – therefore we shall start with describing criteria (with *TI* in the back of our minds already of course).

6.1 CSIRT Statement Properties

When talking about criteria for CSIRTs it needs stating at this stage that these criteria will be based on CSIRT statements (passive or active). And these CSIRT statements have three properties that we want to distinguish between here:

- Authenticity
- Actuality
- Correctness

Authenticity means that we can be sure the statements came from the CSIRT and/or its parent organisation. We include *integrity* of information (the unmodified transfer from one party to another) along that path of course: if the integrity of information is not assured then its authenticity is meaningless.

Actuality means that the statements reflect the current state of affairs, and not one of a past long forgotten. Actuality can only be achieved when statements are maintained: *maintenance* and *actuality* are two sides of the same coin.

Correctness means that the statements are more than authentic and actual: they are met by reality. This can only be checked by – essentially – performance or quality *measurements* of a CSIRTs work. In certification processes of CSIRTs correctness of information would play a major role.

*For **TI** purposes we shall concentrate on the **authenticity** and **actuality** properties of CSIRT statements alone: to also check **correctness** would be to attempt some sort of certification which is way beyond scope [8]. We are convinced that certification of CSIRTs **will** take place in some shape in future, but for the coming few years it is clearly a bridge too far: the CSIRT scene is still far too young to bear rigid schemes of this kind.*

6.2 TI CSIRT-levels

Of course the CSIRT phases recognized in preceding chapters **are** a convenient way to categorize whether a CSIRT is still in its infancy or whether it has already matured and

8 Numerous discussions within the community of CSIRTs have shown to the authors, that certification is not well received by the majority of teams. It will take more time to convince especially teams not coming from a business environment, where service level agreements are fundamental to any service offer, to realize the business need. On the other hand, especially in the research and educational environment, there **seems** to be no need from the constituency, to negotiate service level agreements with CSIRTs – our comment would be: maybe not yet, but the need will no doubt arise there as well.

become accepted. So if the phase scheme is subjective for *TI* purposes, as we argued above, we should replace it by an objective scheme which **does** suit *TI* purposes. Such a scheme can only be based on the information about a CSIRT availavable to TI, and the authenticity of that information. We propose the following scheme, where CSIRTs belong to one of three levels:

- **Level 0:** Information about the CSIRT is available which indicates that the team is within the scope of *TI*.
- **Level 1:** The CSIRT is in the pre-level-2 phase of *TI*, with only 2 possible outcomes: upgrade to Level 2, or fallback to Level 0 after a limited period of time.
- **Level 2:** Information about the CSIRT is available verifiably obtained from individuals verifiably representing the team, thus ensuring[9] *authenticity*. The team participates in *TI*.

Terms like “verifiably” scream for a practical approach towards the problem. We shall therefore propose a possible implementation for these levels now:

Level 2 teams - Information is obtained by:

- Direct contact with an individual from the team and/or its parent organization that can prove the facts about the team is established. At least the personal ID is checked and the individual can prove his/her right to represent the team and/or its parent organization.
- Direct contact is established during a site visit. At least the personal ID of one team and/or parent organization representative is checked and the individual can prove his/her right to represent the team and/or its parent organization.

During the direct contact *TI* MUST log the person's names, ID numbers, nationality together with a written copy of the basic set of information as defined in Appendix E (further explained below), signed by the person the contact is established with. The log MUST be archived by *TI*.

Level 0 teams:

All other teams except Level 1 teams will be listed as "Level 0" based on the information derived from other sources, like:

- News about a new team spread in the community.
- Informal (for example by unsigned email, with simple letterhead) information is received directly from the team. A copy of such information might be provided by another party.

[9] „ensuring“ in this report should always be read statistically, i.e. if something is ensured, there is a high probability – definiton of „high“ deducible from the context - that it is so: in matters of security there is no such thing as absolute certainity (if there ever is)

Essentially, to *TI*, this information is all of the “useful rumour” type. *TI* MUST archive a “written” record, which information was the cause to include a previously unknown team in the list of "level 0" teams.

Level 1 teams:

Level 1 can only be entered from Level 0 (fallback from Level 2 goes directly to Level 0). The way to enter Level is only by means of an invitation from *TI*. That invitation is triggered by a formal (e-mail digitally signed by a person whose key can be verified, formal letterhead) request from the team, its constituency, a Level 2 team, or by *TI* itself. This is further detailed below in the *TI* process description, under Task 2.

A copy of all requests, invitations and reactions with regards to the Level 1 phase MUST be archived by *TI*.

6.3 Criteria

When a CSIRT goes through the *TI* program, moving from level 0 to level 2, it has to face the following criteria. The MUSTS are criteria which have to be met to succesfully pass the program, the SHOULDS are strong recommendations (MUST and SHOULD according to IETF standards, see appendix D).

i. Teams MUST be described by qualitative and a minimum level of quantitative values (basic set of information and services offered) as per Appendix E. This basic set of information is derived from the following sources but was extended considerably to facilitate the purpose of *TI*:
   a) Templates for European Teams:
      – Informal template of FIRST Special Interest Group Europe, 1994
      – EuroCERT template, 1997
   b) FIRST Member/Liaison Profile [FIRST 1999]
   c) Some details taken from the template defined in [RFC2350]

   Teams MUST cooperate with the publication of the delivered data on a *TI* related **restricted-access** website.[10]

ii. Teams MUST cooperate with the publication of the essentials of their contact information on a *TI* related **public** website. The treatment of teams of “level 2 standing” that however have reasons to refuse public exposure, but do want to reach out to their fellow teams, is for further study. [11]

iii. Teams SHOULD present their service to the outside world as per [RFC 2350], including a specification of quantitative values (advanced set of information).[12] The table of content of the advanced set of information is given in Appendix A.

---

10 Access is restricted to level 2 teams and TI entities.

11 A possibility is to treat such „hidden teams“ as Level 0 teams and only classify them on the restricted-access website, not on the public website.

12 Teams that have choosen to provide such documents to the community are for example: DaimlerCrysler's CSIRT service offer (DCERT, http://www.dcert.de) or TeleDanmark's CSIRT service offer (CSIRT.DK, http://www.csirt.dk).

- Teams are advised to model their service descriptions as indicated in appendix B, before attempting to fill in RFC 2350. Any quality assurance parameters set when applying appendix B should be reflected as service level statements inside the RFC 2350 description.
- Teams MUST adhere to their description as per [RFC 2350] including all service level statements therein – if existent.

iv. Teams MUST actively support the *TI* requirement to keep the information they provided to *TI* up-to-date, that is to ensure the *actuality* of the sent-in templates etc. This criteria of *actuality* maintenance also applies to SHOULD criteria, if the CSIRT has chosen to follow those should's and send in the related information – noblesse oblige: if extra information – in itself praiseworthy – becomes unreliable information, then it will turn against itself and defeat the reliability of even the good information.

v. Teams MUST handle all sensitive or private information sent to them – including all incident related information - in a secure and protective way (subject to local law), internally but also when sending it out again. Teams MUST describe their modus operandi in that respect. Teams are advised to establish a secure communications scheme based on PGP or S/MIME in order to help meet that goal.

vi. Teams MUST support QA sessions (per e-mail in principle) with *TI* to clear problems or questions arising with regards to the provided information, its *authenticity* or its *actuality*.

vii. Teams MUST support (not financially) a site visit under the *TI* program if *TI* concludes that a site visit is necessary. [13] Site visits are last-resort possibilities if QA sessions fail or when other pressing reasons exist – but a site visit can also be invited. At a site visit *TI* will naturally limit its scope to the criteria described here – no extra criteria will be set, for that would inevitably lead towards an attempt at certification, which is out of scope. Observations made during the site visit on the process of acquisition of the team's statements with regards to the criteria described here, will be journalled by *TI* objectively.

viii. Teams SHOULD attend FIRST conferences and *TI* supported CSIRT meetings.

[13] Later on we shall see that *TI* should have a review board existing of representatives of Level 2 CSIRTs to decide on such matters

7 The process of *TI*

We shall not describe *TI* as a formal process, but rather mention the main tasks inside the whole process – or perhaps rather, inside the *TI program*, since process for some means a logical stream of events going from i to f , with a fully recognized pathway (with or without multiple tracks, shortcuts and feedbacks) all along the way. *TI* is not helped with such a mathematical description, but a rather more flexible approach is needed.

Within the main tasks the above defined levels and criteria obviously play a major role – they are the vehicles that must ensure the objectivity of *TI*'s proceedings and deliverables. Please note that some subtasks of *TI* (MUSTs and SHOULDs) are already defined within those levels and criteria.

TI's main 4 tasks are as follows:

7.1 TASK 1 : CSIRT Level 0 Reconnaisance

TI MUST undertake an initial effort to recognize CSIRTs that are within *TI* scope. There are some obvious sources for this effort, like the ex-EuroCERT teamstore, FIRST member lists, the halfway 2000 to be published thesis [Kossakowski 1999] and other sources like personal archives.

The thus recognized CSIRTs are automatically listed as Level 0 teams. *TI* MUST store the recognized teams with relevant data (as far as known) like especially e-mail address and suspected constituency, on its website – clearly these data are of best-effort type given the nature of Level 0.

TI *MUST* entertain a low-level background effort to maintain the level 0 list: new teams may be added, disfunctional ones removed. Upgrades to Level 1 and 2 however fall under the following tasks.

It is clear that the recognition and maintenance effort described in this task can be done quite easily and effectively by people or groups of people inside the web-of-trust and well acquainted with the CSIRT scene – whereas relative outsiders would have to invest quite a lot of effort to obtain the same result. This is one of many instances that prove that TI needs an implementation within the scene.

Task 1 involves none of the above defined criteria – since these define actions or stances by CSIRTs, and direct CSIRT effort is not involved in Level 0. However, clearly one of TI's task is to advertize what it stands for, so we derive an additional subtask here:

TI MUST advertize its program on its public website, explaining purpose and proceedings (level 1 and 2 establishment, maintenance etc.) and giving all relevant material like Appendix E, filled-in examples, references to CSIRT Handbook [West-Brown et al. 1998] and other literature etc.

Furthermore *TI* SHOULD advertize the above also on relevant events of TERENA, FIRST, in articles, seminars, conferences. To be succesful this SHOULD really should be a MUST, were it not that the extent in which this takes place rather depends on the party involved in performing *TI*, and the amount of funding available. *This is another instance that proves that TI's (cost-)effectiveness is greatly enhanced when operated within the scene.* Whatever the implementation, there is however one "MUST" that stands out among all "SHOULDS":

TI MUST move regularly within the CSIRT scene – meaning that TI individuals personally communicate with CSIRT (ISP, vendor, government, …) individuals – in order to keep in touch with the current "level 0" and "level 1 and 2 to be" situation.

7.2 TASK 2 : Establishment of Level 1 CSIRTs

Level 1 is a temporary intermediate stage between Levels 0 and 2 – the only two steady state levels. If a team is "level 2 material" than it can upgrade from Level 0 to Level 1 – with the sole intention to make it Level 2 within a fixed period of time – say 3 months. If within that period Level 2 has not been reached, the team automatically falls back to Level 0.

TI MUST invite suitable teams to enter Level 1. The suitability of a team is not the result of a test of some kind – a team's suitability here is already [14] established when:

- A team formally (e-mail digitally signed by a person whose key can be verified, formal letterhead) requires level 2 status from *TI*
- An official representing the teams constituency formally (see above) asks *TI* that "their" team acquire level 2 status
- A level 2 team formally (see above) asks *TI* that another team acquires level 2 status
- TI itself judges that level 2 status is due for a team

Clearly, in the latter 3 cases, TI will first have to establish whether the team is indeed interested in acquiring level 2 status, before sending the formal invitation.

TI's invitation MUST have the form of a formal letter stating the intentions of Level 1 and 2, the exact process to follow, the timeframe and a contact person ("introducer") to accompany the process. The 8 criteria defined above will have to be explained, together with MUST and SHOULD status and the method of verification followed by *TI* (described above under Level 2 explanation).

The process that the team will have to go through will in essence prescribe the implementation of criteria i (filled in template according to Appendix E) and vi (secure e-mail facilitation; key establishment), prescribe support of criteria ii (teamdata on public *TI* website), iv (maintenance of all data), v (support of site visit under circumstances) and vii (e-mail QA sessions with *TI* under circumstances), and encourage adherence to should-criteria iii (RFC 2350 adherence) and viii (visits to relevant *TI* workshops and FIRST conferences).

---

[14] If this liberal attitude would lead to a too big number of Level 2 candidates with a too small percentage of success (big reflux to Level 0) then a more stringent approach may be necessary to reduce the effort involved by *TI* . Such an approach may be either to introduce extra conditions – like an already correctly filled in Template E when applying for Level 1/2 status – or an administrative fee. The latter can only be used when *TI* has acquired a good reputation and teams will actually **want** to register there.

The timeframe given to the team to reach Level 2 status is suggested to be 3 months initially, to be prolongued no more than twice with a period of one month if so requested by the team and approved by *TI*. If this timeframe is not met, the team automatically reverts to Level 0. Any renewed requests for Level 1/2 status will not be taken up in the 6 months following the change back to Level 0.[15]

7.3 TASK 3 : Establishment of Level 2 CSIRTs

Following the Level 1 establishment process described above, the team will start meeting at least the "MUST" criteria. In order to do that it will send in data to *TI* like filled-in Appendix E, PGP keys etc. – these data will have to be provided on the trusted Level 2 *as described above under the explanation of Level 2*, essentially meaning that their authenticity (and integrity) is verifiably guaranteed by somebody whose "personal ID has been checked **and** who can prove his/her right to represent the team and/or its parent organization".

If the team then meets all "MUSTS" within the given timeframe, and the Level 2 trusted verification of all data provided has proven okay, then TI MUST upgrade the team's status to Level 2 and notify the team and other Level 2 teams thereof.

TI MUST ensure that all data about Level 2 teams (filled in Appendix E, relevant crypto keys, public contact information, hyperlinks, and – if applicable – RFC 2350 or other additional information) as provided by the teams themselves are available on the restricted *TI* website (the public info of course being on the public *TI* website). Maintenance and expiry of info as per task number 4.

TI MUST also ensure that for every Level 2 team TI states how the information involved was originally gathered, compiled and verified (including the identity and status of the authenticator from the team and the person involved in its TI role) – plus giving possible additional relevant OBJECTIVE remarks. This extra information serves the purpose of enabling other Level 2 teams of making their own qualitative assessment regarding the information available about a team. *The essence here is that it is not TI who decides whether a team joins the web-of-trust, but that it's the teams themselves that decide about that – Level 2 status means having fulfilled several formal duties making it **easy** to enter Phase IIIb, the web-of-trust inmate phase – but it's not a guarantee: trust cannot be bought, it can only be earned.*

7.4 TASK 4 : Maintenance of Level 2 Status

As sometimes changes will not only impact the team's staff, or its structure, but also service levels, constituency definition, contact data, etc, a one time only Level 2 verification is simply not enough: the Level 2 status requires maintenance. The teams already know about that, since the maintenance requirement is one of the criteria (i.e. iv) they had to agree on when acquiring Level 2 status.

[15] Unless the *TI review board* decides to make an exception: the review board is introduced later on

Polled by *TI*, it is assumed that the current available information is still current. To ensure this, the following approach is taken:

- The information available and published about any team MUST be verified at least every four months by a joint effort of team and *TI*. The verification is based on status updates / acknowledgements from the team.

- A team in Level 2 MUST at least reply to *TI* requests regarding their status in order to maintain their Level 2 status as per criteria vii. Moreover, they are expected to behave more actively as per criteria iv and perform as mentioned below:

- A team MUST inform *TI* about any change that relates to contact or public key information within two weeks and provide the appropriate corrections. If public key information is changing, the team SHOULD provide appropriate key revocation information.

- A team MUST inform *TI* about changes that deeply impact their establishment within one month and describe the approach taken to further provide its function:
  - Changes within personnel
  - Changes within funding
  - Constituency changes

- A team SHOULD inform *TI* about other changes within the published report (notably the filled-in Appendix E, public contact info, availability of hyperlinks and such) within eight weeks.

- TI MUST react to complaints or reports about level 2 teams when these complains/reports come from level 2 teams. All other sources of information are regarded non-authoritative and the information handled accordingly.

TI MUST maintain an archive containing requests, acknowledgments and other communication that results into changes of the team's information. Whenever information is not exchanged electronically, a paper copy MUST be archived or in case of a verbal / telephone conversion, a written or electronic copy MUST be created and archived.

If a team does verifiably not comply with the above rules and does not react to subsequent *TI* requests, stating this fact and given a 2 months deadline, within that period of 2 months or fails to provide due content and authentication, then *TI* MUST give the team formal notice (by signed mail and written letter) that their Level 2 status will expire within 2 months. *TI* will publish the expiry date on the restricted website together with the team's data. If the team does not react within that second 2 months period or fails to provide due content and authentication, then *TI* MUST revert the team to Level 0 status, and inform all Level 2 teams.[16] This change will also be reflected on the public web site.

The above sanction process is a very dry administrative one, agreed. However, it is the only feasible process, as *TI* has no authority whatsoever over any team or their interactions and trust relationships. *TI*'s sole purpose is to distribute correct statements. However, as known, these statements do not only give specific details but also allow an assessment of the value

[16] Only the later-to-be-introduced *TI review board* can make positive or negative exceptions to this rule

of these details, since TI is also tasked to give information about the collection and verification of data. The assessment of those data is carried out by the information receivers i.e. the Level 2 teams, not by *TI*, who retains its objectivity at all times.[17]

However, the afore mentioned assessment may mean that even in circumstances where the official status of a team is still Level 2, the other Level 2 teams may still perceive a problem. An example will best clarify that:

> Example: A team loses almost all of its members due to better offers from private industry. The management of the team decides to hide this fact as long as possible and to work best effort – but are hopelessly understaffed and doing a lousy job. After five weeks another team notices that no e-mail is answered and reports this to the *TI*. After investigating this issue, the situation becomes obvious and is documented "AS IS", revealing the wrong management decision.

In a strange situation like that, with a big problem within a Level 2 team revealed, the below introduced *TI review board* can take actions like making enquiries or changing the team's status. *TI* itself can only go by the book, or it will lose its credibility as an objective party.

7.5 TI internationally

Clearly TI is not intended to make Europe a CSIRT island, entirely of itself, to paraphrase John Donne. TI is intended to ease the task of new CSIRTs to enter the web-of-trust, and to help maintain that web of trust.

The trust relationships between European teams working together with TI, and other teams, both outside Europe, but also inside Europe but not working with TI – is primarily a matter for the teams themselves.

It is however clear that TI should liaise with at least a few key teams around the world, to enhance its worth and to gauge the TI program with the best practices elsewhere. Examples of such key teams could be CERT/CC, CIAC, AUSCERT and others. It would be recommendable to investigate the possibility to also classify those teams as Level 2 teams, or perhaps "associate" Level 2 teams.

Additional to this TI should obviously liaise with the only professional organisation for CERT teams in the world, i.e. the FIRST.

7.6 TI Review Board

To be able to review the operation of *TI*, a board of representatives of level 2 teams MUST be established. This board will review the operation of *TI* and address all special issues that might result from its operation. It is henceforth called *TI review board*. The board will perform the following tasks:

[17] Nevertheless *TI* has substantial influence as others will implicitly "trust" the team based on the information available. Therefore it is highly recommended to review and oversee the task of *TI* carefully.

- Receive trimester reports by *TI*.
- Review the overall performance of *TI* and handle all complaints about its function
- Sign the PGP keys of *TI* to foster the authenticity of these keys
- Set and change the operational framework for *TI* as originally based on this report
- Decide about special issues with regards to Level 1 and 2 status, like making exceptions to the set *TI* rules for Level changes (1 to 2, or 2 to 0), deciding on a site visit to clear issues not clearable otherwise, etc.

To be able to carry out these responsibilities, it is expected, that one yearly face-to-face meeting (or videoconferencing alternative) is necessary. To allow day-to-day communication, the establishment of a mailing list and the use of PGP or S/MIME to ensure confidentiality and authenticity is expected to satisfy all needs. The board has the right to review the archive maintained by *TI* at any time to clarify any complaints about *TI* directed to the board and to be able to review overall performance.

The establishment of the board itself depends on the implementation model of *TI*. A review of that follows in the next chapter. In essence, the board could be either appointed (by the main funding party of *TI*) or elected (if several more or less equal funding parties exist).

8 Implementation Review

After having described the *TI* process and underlying criteria at great length, we shall now review the possibilities of *TI* implementation. We shall start with investigating the possibility to have TI entertained by existing or potential introducing functions – conclude that that is not a viable approach and then looking at possibilities to implement *TI* in another setting.

8.1 Review of today's available Introducing Functions

In the beginning of this report, today's available functions that introduce teams to each other were already alluded to. After having developed the *TI* function, we shall shortly review these existing functions now to show, that they are currently not able to emulate *TI*.

8.1.1 FIRST - Forum of Incident Response and Security Teams

Established in 1990 by 12 incident response teams, most of them in the USA, FIRST today consists of nearly 90 international teams. Members are introduced by a sponsor and are accepted by a vote of the Steering Committee.[18]

Depending on the effort, the sponsor is spending in working with the applying team, authenticity can generally be assumed, but is not guaranteed. Although a defined set of information is requested in order to apply for membership, it does not require to provide for example the RFC 2350 compliant information or any specific information regarding the service.

Without mandatory criteria and standardized processes, that must be followed by sponsors and applying teams, there is no certain categorization of (new and old) members.

Conclusion: There exists no mapping between FIRST members and the scheme developed in this report. The sponsorship process of FIRST is not suitable to serve as prototype for *TI* without fundamental changes. Therefore the current FIRST model does not suit *TI* needs at all.

8.1.2 European CERT Coordination Center (EuroCERT)

As the setup of the EuroCERT service was designed to facilitate only the operation of the funding member organizations, the introducing into the society of European incident response teams was done on an informal basis only. The information collected about single teams were distributed via a collection of web pages. It only covered part of the information defined as basic set of information (Appendix E).

Conclusion: Regardless of the fact, that the EuroCERT service was suspended, the information about European teams is by no means complete to serve as basis for a trusted interaction among teams. Although a function similar to *TI* was envisioned in the CERT Task Force Report [TERENA TF CERIE 1995], the overall restriction to funding members

[18] 10 individuals are elected by the membership to serve for a two year term. The task of the SC is to facilitate the development of the organization and to handle the day to day operations.

denies a broader coverage of European teams, which is necessary to enable the building of a trusted web of CSIRTs.

8.1.3 Cooperation of several CSIRTs (a.k.a. Special Interest Group Europe)

Before the EuroCERT service was established, the European teams met due to the efforts of individuals of long time established teams since late 1993. During the second meeting the participating teams agreed on a set of information that should be made available by all teams to support a better cooperation. This information template was used as basis for the information maintained by the EuroCERT service later.

Conclusion: As the information provided by the teams was by no means authenticated or centrally maintained, there was no "service" offer. This approach lacks the fundamental characteristics that were the driving force to develop the function of *TI*.

8.2 Review of potentially available Introducing Functions

Potential (near future) candidates to harbour *TI* are now evaluated:

8.2.1 FIRST - Forum of Incident Response and Security Teams

Although it would be very attractive to benefit from the international coverage if FIRST would provide *TI*, it is unlikely that FIRST will adopt the task as described in this report within short term. The reasons for this assessment are that FIRST currently does not support any operational services at all [19], and that FIRST is entangled in a struggle to grow from its volunteer based past into a professional funded organisation which will take at least till 2001.

8.2.2 TERENA - Trans-European Research and Education Networking Association

Although TERENA has well established (legal and operational) relationships to European research network organizations, it provides mechanisms to deal with authentication mainly within this realm. This does not necessarily include commercial network organizations or (multi) national companies, which is the area where many new teams that will be created.

Additionally, as TERENA itself is not involved in incident response, it is currently not directly affiliated with the community. Therefore it is highly unlikely, that it can successfully provide the *TI* function within short term by itself, that is: by the secretariat. Subcontraction of *TI* to a suitable party however is a highly viable approach, as has been argued before.

8.2.3 Informal Cooperation of several CSIRTs

While this approach seems to suitable to be accepted by the incident response community, given that single teams cannot exercise any specific influence, the informal character of such a cooperation would deny the continuity and guaranteed quality necessary to satisfy the requirements of *TI*.

---

19 FIRST has recently put out a Request For Proposals for a (paid) secretariat. No service that would extend the introductional role beyond the actual FIRST members and teams applying for membership was included within the list of services for it.

8.2.4 Subcontraction

If the requirements for the entity, that is selected as subcontractor to provide *TI*, are defined well enough, subcontraction seems the only solution to ensure the desired functionality and exercise quality control. As most of the European teams still are affiliated with research and educational networks, TERENA seems appropriate to coordinate the funding and management tasks involved.

8.3 Requirements for Entities providing TI

In order to provide *TI* in a successful way the entity selected MUST in our opinion have the following attributes:

- Respect within the community.
- International visibility.
- Experiences within FIRST, TERENA and the European community of Computer Security Incident Response Teams.

As a SHOULD we define:

- No conflict of interest by acting as CSIRT for a constituency within the scope of *TI*.
- One identifiable entity providing *TI*, for reasons of flexibility, speed and uniformness – i.e.: **quality** - of the *TI* service.

8.4 TI Information Services

The most visible part of the *TI* program are information sets about various teams. Within the today's Internet, the dissemination of such information is best handled by providing a WWW server.

To facilitate the information dissemination the following functions must be provided:

- All entries[20] for all categories (Level 0 / Level 1 / Level 2) listed
- All entries listed alphabetically
- All entries listed alphabetically for all countries
- A history of changes and additions
- A search function across all pages / all entries
- Policy statements and descriptions of *TI*

It would be useful to provide additional information and especially pointers to useful information on Computer Security Incident Response and activities in this area (meetings, conferences, ...) as the web site will become a focal point for "meta" information on CSIRTs.

To ensure the authenticity of the information, appropriate security mechanisms are important:

- Support of SSL (v3) Client Authentication for any management activities using a web interface.

[20] Each entry consist of the Basic Set of Information as described in Appendix E and pointers to any other information, especially any Advanced Set of Information (the filled out RFC2350 template). To provide a focal point for all information available about teams, copies of the Advanced Set of Information are provided by *TI*.

- Support of SSH (v2) confidentiality and authentication for any other management activities using public network access.
- Support of SSL Server Authentication with a Server Certificate of a well established Certification Authority. Thereby providing users with authentic information from the server.
- Support of PGP signatures for static web pages to enable users to check the authenticity for documents derived from the server. Thereby providing users with additional safeguards against manipulations of documents "on" the server.

As PGP and digital signatures play a vital role not only in protecting specific information but also e-mail communication the relevant PGP keys of *TI* need to be certified by a well established Certification Authority and must be made available on PGP key servers for worldwide access (http://www.pgp.net). It is not necessary to set up a specific PGP key server, although it would provide an efficient way to distribute not only the PGP keys of *TI* but also PGP keys belonging to teams and their team members. The use of S/MIME additional to PGP should be introduced if needed, under the same CA framework.

8.5 Cost Recovery

As the teams that are listed as Level 1 and especially as Level 2 team receive benefits from this listing, it is advisable to recover some of the costs involved to maintain *TI*.

At this early stage only the three following recommendations are made:

- Teams listed as Level 2 teams MUST pay a yearly registration fee. This registration fee should be payed to the organization overseeing *TI*.

- Teams acquiring level 1 and 2 status MUST pay what-it-takes administrative fees to acquire their new status.

- Travel costs that are necessary to facilitate any specific meetings requested by teams striving to obtain (or maintain) Level 2 status SHOULD be reimbursed by the requesting teams. Travel costs for site visits initiated by the *TI review board* occur only in special cases in the interest of the CSIRT community and are not supposed to be reimbursed by the teams visited.

8.6 Future Perspectives

During the first implementation of *TI* it seems not appropriate to rely on external functions to provide the same level of assurance. In future *TI* incarnations such external functions may however ease some of the *TI* tasks. Three strategies seem most promising in this respect:

- **Use of Public Key Infrastructures:**
  Instead of relying on personal meetings or site visits the authenticity of information received about teams can be assured by digital signatures. To establish the same level of authenticity, only digital signatures that are based on keys certified by Certification

Authorities that require personal picture IDs in order to verify the key owner, are acceptable.[21]
It is necessary to list all Certification Authorities whose certificates are accepted.

- **Acceptance of "Associated" Introducer:**
  If other forum organizations (like FIRST) provide a compatible set of information about their members, the membership can be recognized to qualify the team as Level 1 team. An even more advanced approach would be to accept a forum organization a so called "associated" introducer. To establish the same level of authenticity as provided by *TI*, any "associated" introducer" needs to take similar measures to ensure the authenticity of their members.

- **Decentralization of some *TI* tasks:**
  Whenever teams have a long term affiliation with the European community of incident response teams like CERT-NL and DFN-CERT, they could as well function as liaison for *TI*. To do so, they would need to adhere to exactly the same rules and standards, since they would be a stand-in for *TI*. *TI* would need to enforce quality assurance and control their work. While this could be a workable solution, it greatly depends on individuals within the team.[22] Apart from that, this extra work for the teams would clearly go beyond the possibilities of tollfree work, so would have to be funded. The people inside the teams don't come at a lower cost than *TI* people. That, plus the control function needed at *TI* and the extra overhead make it highly unlikely that this would be a cost-effective possibility.

[21] For example the DFN-PCA (http://www.pca.dfn.de/dfnpca) operates a Certification Authority that provides this check prior to certifying a public key (PGP, PEM).

[22] Personnel changeover is always one of the most obvious challenges for the continuity of service offers. It applies as well for the trusted introducer as for any incident response team.

9 Outlook and Recommendations

The replacement of trust by expectations based on authenticated information is the main purpose of *TI*. To facilitate this change of behaviour on the side of information "consumers" - be it a CSIRT or a site administrator that wants to report an incident - *TI* is designed to describe teams, checking on the authenticity of this information, maintain its actuality and disseminate this information to the public. In addition more detailed information will be made available to recognized CSIRTs.

Overall, the *TI* approach will provide the European teams with one critical part of an evolving international infrastructure for security incident response. As trust will still play a role within the interrelationship and cooperation among European CSIRTs, the availability of a "trusted" third party - *TI* - will help to identify, followup and resolve even dramatic changes within single teams, for example the changeover related to a complete re-newal of all employees. Although *TI* cannot change the course of events, it allows other CSIRTs to base their assessments, how capable a team is and what expectations are reasonable, on more objective information than is available today.

Based on the function as clearing house of teams and introducer of new teams other functions might be suitable, depending on the additional expertise available within the *TI* team. Clearly, to act as a mentor for a new team for example will involve much more than is necessary to carry out *TI* itself. But as it was highlighted while reviewing the requirements to implement *TI*, the involvement with incident response and intimate knowledge of the international and European community is mandatory to carry out *TI* successfully. It is expected, that *TI* would become a focal point for the further development of incident response in Europe.

The implicite support of the establishment of new teams and the explicitly designed integration within the infrastructure of existing teams will raise the awareness of their very existence. This will also enable the public recognition of the need for global security incident response and the need for European coordination of the Europe based infrastructure components. It will also allow the CSIRT community to discuss questions that are relevant for the community, like: How a European coordination should look like? What issues need to be covered when defining interactions?

We recommend to review the proposed *TI* process and the criteria it will be based on for a limited stretch of time. Thereafter any changes identified during the discussions should be incorporated. The result should then serve as the basis for a *TI* implementation.

10 References

- [FIRST 1999] FIRST Member/Liaison Profile / Forum of Incident Response and Security Teams. - Version 2. - http://www.first.org/docs/profile.txt
- [Kossakowski et al. 1999] Responding to Intrusions / Klaus-Peter Kossakowski ; Julia Allen ; Christopher Alberts ; Cory Cohen ; Gary Ford ; Barbara Fraser ; Eric Hayes ; John Kochmar ; Suresh Konda ; William Wilson. - Security Improvement Module CMU/SEI-SIM-006. - Pittsburgh, PA: Carnegie Mellon University, 1999.
- [Kossakowski 1999] Information Technology Incident Response Capabilities / Klaus-Peter Kossakowski. - University of Hamburg, Computer Science Department, 1999. - Doktor thesis. - Work in Progress.
- [RFC2119] Key words for use in RFCs to Indicate Requirement Levels / Scott Bradner. - Request For Comments 2119.
- [RFC2350] Expectations for Computer Security Incident Response / Nevil Brownlee ; Erik Guttman. - Request For Comments 2350.
- [TERENA TF CERIE 1995] CERTs in Europe / Joao Nuno Ferreira, Alf Hansen, Tomaz Klobucar, Klaus-Peter Kossakowski, Manuel Medina, Damir Rajnovic, Olaf Schjelderup, Don Stikvoort. - Final Report. - October 1995.
- [West-Brown et al. 1998] Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J. West-Brown ; Don Stikvoort ; Klaus-Peter Kossakowski. - CMU/SEI-98-HB-001. - Pittsburgh, PA: Carnegie Mellon University, 1998.
- [West-Brown, Kossakowski 1999] International Infrastructure for Global Security Incident Response / Moira J. West-Brown ; Klaus-Peter Kossakowski. - Pittsburgh, PA: Carnegie Mellon University, 1999.

11 Abbreviations

CA:	Certification Authority
CERT:	Previously used as common term for Computer Security Incident Response Teams (CSIRTs), "short" name of the CERT Coordination Center, established in 1988 at the Carnegie Mellon University, Pittsburgh, PA.
CSIRT:	Computer Security Incident Response Team
FIRST:	Forum of Incident Response and Security Teams, international forum organization for CSIRTs and security teams, established in 1990.
GRIP:	Guidelines and Recommendations for Incident Processing, an IETF working group, established in 1995.
IETF:	Internet Engineering Task Force
IP:	Internet Protocol
PCA:	Policy Certification Authority
PEM:	Privacy Enhanced Mail
PGP:	Pretty Good Privacy
RFC:	Request of Comments
RIPE NCC:	RIPE Network Coordination Center (gives out IP numbers in Europe, maintains RIPE database etc.) – society with paying members
RIPE:	Réseaux IP Européennes, informal gathering of IP providers and interested organisations in Europe aiming at coordination of IP issues
SSH:	Secure Shell
SSL:	Secure Socket Layer
TERENA:	Trans-European Research and Education Networking Association
WWW:	World Wide Web

Appendix A:
Structure of CSIRT Public Statement according to [RFC 2350]

1. Document Information

1.1 Date of Last Update
1.2 Distribution List for Notifications
1.3 Locations where this Document May Be Found

2. Contact Information

2.1 Name of the Team
2.2 Address
2.3 Time Zone
2.4 Telephone Number
2.5 Facsimile Number
2.6 Other Telecommunication
2.7 Electronic Mail Address
2.8 Public Keys and Encryption Information
2.9 Team Members
2.10 Other Information
2.11 Points of Customer Contact

3. Charter

3.1 Mission Statement
3.2 Constituency
3.3 Sponsorship and/or Affiliation
3.4 Authority

4. Policies

4.1 Types of Incidents and Level of Support
4.2 Co-operation, Interaction and Disclosure of Information
4.3 Communication and Authentication

5. Services

5.1 Incident Response
5.2 Proactive Activities

6. Incident Reporting Forms

7. Disclaimer

Appendix B:
Service Description Attributes according to [West et al. 1998]

Objective

Purpose and nature of the service.

Definitions

Description of scope and depth of service.

Function Descriptions

Descriptions of individual functions within the service.

Availability

The conditions under which the service is available: to whom, when and how.

Quality Assurance

Quality assurance parameters applicable for the service. Includes both setting and limiting of constituency expectations.

Interactions and Information Disclosure

The interactions between the CSIRT and parties affected by the service, such as the constituency, other teams, and the media. Includes setting informatoin requirements for parties accessing the service, and defining the strategy with regards to the disclosure of information (both restricted and public).

Interfaces with Other Services

Define and specify the information flow exchange points between this service and other CSIRT services it interacts with.

Priority

The relative priorities of functions within the service, and of the service versus other CSIRT services.

Appendix C:
Key elements of an international infrastructure for global IT security incident response
[West, Kossakowski 1999]

An Infrastructure

To enable and coordinate increasingly effective global security incident response efforts to provide a higher level of response capabilities (early warnings, trends, predictive information).

Mission statement:
Provide effective and comprehensive global response to IT security response on a local, national and international scale by:

- Providing an infrastructure to enable and coordinate global incident response efforts;
- Coordinating activities of incident response and security teams throughout the world; and
- Supporting the formation, operation and integration of incident response and security teams into the global security incident response infrastructure.

A Forum

To facilitate the discussion and development of international standards, policies, and agreements that support global security incident response.

Mission statement:
Provide an open forum for law enforcement, policy makers, technology developers, incident response and security teams and practicioners to improve IT security and global security incident response on a local, national and international scale by:

- Fostering the exchange of information and innovation;
- Improving policies and practice by identifying and addressing IT security and global incident response issues; and
- Promoting IT security and global security incident response issues for the benefit of humanity.

A Capability

To support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community.

Mission statement:

Provide accurate and timely information covering all aspects of IT security and global incident response activities which are of interest on a local, national and international scale by:

- Acting as a clearing house and distribution center for sanitized information from the global incident response infrastructure and
- Providing a global perspective of the state of the threat by collecting and analyzing available incident related data from all available sources.

A Professional Organization

To enhance the recognition and education of incident response and information technology security personnel and teams.

Mission statement:
To promote and support the field and practice of incident response activities on a local, national and international scale by:

- Promoting and enhancing the image and status of the incident response and security team community;
- Setting and upholding standards for the incident response and security team profession and community; and
- Supporting the development and improvement of the global incident response infrastructure.

Appendix D:
Standard definitions taken from the IETF approach [RFC2119]

MUST
This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification..

SHOULD
This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

Appendix E:
Basic Set of Information

The basic set of information consists of three parts, one mandatory and one optional part are related to the team itself, the other mandatory part is related to the task of *TI*.

Mandatory Fields describing the Team

Team Name

Official team name
Short team name (Acronym)
Host organization (if the team is decentralised, list all host organizations)
Country the team is located in (if multiple offices exist, list all countries)
Date of establishment

Constituency

Type of constituency (vendor customer base, internal to host organization, ISP customer base, ...)
Description of constituency
Internet domain and/or IP address information describing the constituency
All countries in which constituency members are located in

Team Contact Information

Regular telephone number (country code, telephone number, timezone relative to GMT)
Emergency telephone number (country code, telephone number, timezone relative to GMT)
Email address
Facsimile number (country code, telefax number)
Other telecommunication facilities
Postal address

Team Representative

Name of person representing the team
Contact information

References

Track record of working relationships with other teams

Services

Specify available reactive services, using the following list (or adding to it):
- vulnerability analysis
- critter analysis

- forensic analysis
- incident response
- incident response support
- incident response coordination
- vulnerability response coordination

Specify available proactive services, using the following list (or adding to it):

- announcements (intrusion and vulnerability warnings and advisories)
- technology watch
- security audit
- trend and neighbourhood watch
- configuration/maintenance of security tools
- development of security tools
- provision of intrusion detection services

Specify security quality management services, using the following list (or adding to it):

- risk analysis
- business continuity planning
- security consulting
- awareness building
- training
- product evaluation
- provision of intrusion detection services

Information handling policy

How is incoming information “tagged” or “classified”?
How is information handled, especially with regards to exclusivity?
What considerations are adopted for the disclosure of information (“when what?”), especially incident related information passed on to other teams or to sites?
Are there legal considerations to take into account with regards to the information handling?

Cryptography

Policy on use of cryptography to shield exclusivity&integrity in archives and/or in datacommunication, especially e-mail.
This policy must include possible legal boundary conditions as key escrow or enforceability of decryption in case of lawsuits.
If encrypted e-mail is possible, then at least provide:
PGP[23] key of Team Representative;
PGP key of Team.
Provision of X.509 certificates (for S/MIME and other purposes) is optional.

Optional Fields describing the Team

Team Members

[23] For all practical considerations PGP (Pretty Good Privacy) is the established standard for providing confidential and authentic communication within the Internet. Whenever other cryptographic applications will be used, the same scheme can be applied without fundamental changes.

Names, contact information and PGP keys of other team members

Business Hours

Description of business hours
Procedures for contacting the teams outside business hours

Technical Expertise

Operating Systems
System Platforms
Networks
...

Contact Information for Constituency / Host Organization

Contact information for person/organization representing the constituency
Contact information for person representing the host organization

PGP Key Revocation Certificates

Key Revocation Certificates for previously distributed PGP keys

Information Server

WWW server
Mailing lists
(Anon)FTP server
NetNews
...

FIRST Membership

Membership status (FIRST member/Liaison)
Date of membership approval

Mandatory Fields describing the actions of *TI*

Classification

Actual classification (Known / Level 1 / Level 2)
Date of first classification
Date of last classification change
Previous classification (Known / Level 1 / Level 2)
Reason for last classification change

Status Updates

Date of last verification
Method of last verification
Date of last change announcement received from the team

Open Issues

List of open issues (date of issue recognized, description, approach taken)

History

List of all actions carried out in regard to the mandatory and optional fields describing the team (for each action the entry will give date and person)