TERENA Task Force

CERTs in Europe

Final Report, October 1995[1]

Abstract

Since the first Computer Emergency Response Team (CERT) emerged as a result of the Internet worm of November 1988 many other teams have been formed. The concept of these teams which help a specific user community in cases of computer security incidents has proven to be successful. Because of the ongoing growth of the number of teams there is an increasing need to foster coordination and cooperation inside this community.

FIRST – the Forum of Incident Response and Security Teams – provides an open forum to discuss common problems of existing teams and to exchange information and knowledge related to the tasks of the teams. The CERT Coordination Center (Pittsburgh, PA, USA) has been providing much help to coordinate security incidents with an international scope. Due to the expansion of the Internet, the CERT Coordination Center will not be able to uphold this service for the Internet at large.

Noting the increasing number of teams inside Europe, the problem of cooperation and coordination must be addressed in order to avoid negative effects for the user community and the network as more and more security incidents will occur. To meet this challenge the TERENA Task Force „CERTs in Europe“ analysed the current situation and consequently constructed a coordination model to overcome the shortcomings of the current situation.

This coordination model has been layered into three levels of increasing service:

- Incident Support (1 FTE):
  Support functions are needed to enable cooperation and coordination. Examples of such functions are meetings, contact information, information services, secure communication, promotion. The maintenance of this service can be handled inside business hours.

- Basic Incident Coordination (3 FTE):
  In addition to the Incident Support services this model focuses on the need of incident coordination complementary to the incident handling which is mainly taken care of by the existing teams. Coordinating an incident implies channeling

[1] The work of the task force was carried out from June to October 1995. This report is the product of the whole group: Joao Nuno Ferreira (RCCN, Portugal) Alf Hansen (UNINETT, Norway), Tomaz Klobucar (JSI, Slovenia), Klaus-Peter Kossakowski (University of Hamburg, Germany), Manuel Medina (UPC, Spain), Damir Rajnovic (MST, Croatia), Olaf Schjelderup (UNINETT, Norway) and Don Stikvoort (SURFnet, The Netherlands).

relevant information to the right teams and building the bigger picture to improve quality of service. The expertise, facts and background information gained from the coordination effort should be made available to the client teams. The basic incident coordination service should be available outside business hours as well as inside.

- Full Incident Coordination (5 FTE):
  While all basic services needed to coordinate incidents have been addressed in the previous level of service, extended and additional services are needed in the areas of security vulnerabilities, education and security technologies, in order to allow proper preventive measures and support the technical know-how and work of the coordinated teams. On the longer run this value-added approach will prove to be more effective than just coordinating a random distribution of expertise among teams. The full incident coordination service must be available 24 hours a day, 7 days a week.

An important conclusion of the task force is, that the three service levels described above together provide a model which offers a migration path towards a coordinated infrastructure for computer security incident handling within Europe. No competition to existing teams will arise, on the contrary, existing teams will clearly gain from the proposed infrastructure. In addition it will become much easier for new teams to start participating in the community of existing teams, thus enhancing overall efficiency.

Recommendations

The task force's recommendation is to implement the Basic Incident Coordination service right away. While important parts of the Incident Support service are already being provided through the voluntary work of single teams the coordination issue can only be dealt with in a formalised and funded fashion, due to the resources necessary for this task.

To implement the Basic Incident Coordination service it is appropriate to first take over the Incident Support services scattered over the field. Therefore the task force recommends to start out with one FTE. The task of this person would be to learn from existing teams, take over the voluntarily provided services and add work-items and especially structure while doing so. After a short period (six to nine months) two FTE should be added to allow the setup of the team and – after additional education and training – to enable the team to become fully operational.

It is further recommended to review the results of this service implementation after its first year of full operation, to decide on how to progress towards Full Incident Coordination. This progress can be a gradual process.

In this final report the task force goes into the matter described above in more depth and detail.

1 Introduction

Millions of people use data-exchange networks today. The Internet is the most famous example. "Use" is unavoidably coupled to "abuse". Thousands of people abuse network facilities for all the common reasons: crime, gain, revenge, or "fun". Thus security measures have to be taken in order to protect data, computers and networks. And increasingly so since the capital investments which depend on information handling systems are exceeding. Security in this area is not easy to achieve because of security's tense relation to ease-of-use and openness – essential characteristics of today's worldwide networks.

To enforce and guard information security all companies, institutions and networks nowadays formulate security policies and install people or teams to maintain these policies. At the network level security teams exist since roughly 1988 inside the Internet. They are often referred to under the single name "CERT" (Computer Emergency Response Team) though there are well over 45 registered independent teams nowadays doing this kind of work. The number of CERTs or IRTs (Incident Response Team – both terms can be used synonymously) is rapidly growing, especially inside Europe. Since coordination between IRTs is absolutely vital when handling security incidents occurring in the global society of networks, the growing number of IRTs causes an increasing coordination problem, not least inside Europe. This problem is apparent for experienced teams and even more so for the novice teams: support for the latter ones should be an integral part of any solution to the coordination problem.

This document aims at explaining the European situation with regard to CERTs and IRTs and presenting a solution for the growing coordination problem, in the form of a pan-European service providing an effective form of coordination for the European CERTs. Chapter 2 explains a suitable model for such a service in detail. Chapter 3 then proposes a strategy to implement this model of CERT coordination. Finally, in chapter 4, suggestions are made on how to proceed with regards to time schedule, setup and funding of the proposed European CERT coordination service.

A more detailed explanation of the current situation now follows.

1.1 Terms and Definitions

Incident Any security incident directly related to computers or networks is labeled "incident" in this document. Spontaneously crashing harddisks, the occurrence of computer viruses, cracking computer systems via the network (often referred to as "hacking"): all are incidents.

Incident Handling Incident handling is the corrective or repressive action taken when an incident occurs. The target of this action is to minimise the effect of the incident and – if applicable – to locate the source of the incident in order to prevent future alike incidents.

Incident Response Team (IRT) When an organisation has put the task of incident handling into the hands of a specific set of people, the latter team is commonly referred to as Incident Response Team or IRT. Universities, network providers, companies, government agencies etc. have been building IRTs since roughly 1988, especially in the USA.

CERT (Computer Emergency Response Team) The original but less accurate term for Incident Response Teams.

Incident Coordination In today's global networks numerous incidents occur which are not bounded by the walls of an institution or LAN. Hence in many cases incidents concern more than just one Incident Response Team. Considering the potential amount of IRTs in e. g. the Internet and considering that the communication between IRTs should be of a trusted nature, the need for some form of coordination is apparent. The most famous example of a team specialising on incident coordination is CERT Coordination Center in Pittsburgh, USA. Commonly referred to as "the" CERT, CERT Coordination Center was founded in 1988 as the incident coordination team for the Internet. Since 1988 however various network providers have built coordinating IRTs, though on a smaller scale, often also copying the acronym CERT (CERT-NL, DFN-CERT, AUSCERT, etc).

FIRST Started in 1990, the Forum of Incident Response and Security Teams brings together a variety of computer security incident response teams from government, commercial, and academic organisations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has over 45 members. Note: FIRST is a forum organisation, it is itself not an IRT, neither does FIRST currently have any active role in incident coordination.

1.2 Security Threats Focus

The scope of even only information security is overwhelming. In this report there is a clear focus on the security of information per se, information flows and information systems, with the exclusion of physical security. Prevention and incident handling in this area are the prime issues.

Furthermore this document focuses on the coordination issue. Though single IRTs might for instance bother with crashing harddisks, this is hardly a topic for IRT coordination. This narrows down the scope to essentially non-isolated problems like viruses, software vulnerabilities, cracking ("hacking") etc.

1.3 Incident Prevention and Handling

The need for incident prevention and the need to handle incidents when they do occur is obvious. The capability of safe information handling is nowadays mission critical, both in the commercial and the academic world. Loss of data or temporary outages of information systems e. g. due to "hacking" cost considerable amounts of money today and can easily ruin firms in certain branches.

1.4 Incident Response Teams

A growing number of companies, universities, networks, etc. has established an Incident Response Team for their specific constituency. These teams are very different in size, scope and organisation, reflecting the differences in constituencies. Company IRTs, for example, tend to both handle and solve incidents, whereas IRTs of network providers often specialise on the coordination issue, their customers doing the hands-on work. There exist teams specialising on viruses, or on Internet security, or on a specific operating system: all depending on their constituency.

The idea of having an IRT for a well defined constituency is generally regarded as a beneficial one, the typical advantages being:

- independence and safety: security is handled within the organisation and not by "outsiders"
- clear authoritative position of IRT within constituency
- usually dealing with national law only
- near to constituency: same language, few cultural differences
- spread over a limited number of time-zones

The coordination issue is dealt with by adopting a hierarchy which is as lean as possible to avoid long communication paths. Take the typical IRT of a network provider as an example. Its constituency is formed by the IRTs and security contacts of its customers, e. g. universities or companies. The constituency of those "local" IRTs on their turn may well be the end-users themselves.

1.5 International Situation

The only existing forum in the world where IRTs meet and exchange information is FIRST. Since incidents usually cross IRT borders, it is crucial that IRTs work together: FIRST is the forum to start off such relations. Another example of FIRST's importance is the vulnerability issue: reports of new vulnerabilities in essential software like operating systems, E-mail handlers, WWW browsers, and reports of new viruses are shared between the FIRST members. This has proven to be an efficient and safe way to get this potentially vital information to the end-user.

Other FIRST activities comprise organising an annual incident handling and security workshop and coordinating issues like secure communication between its members. The best-known members of FIRST are CERT Coordination Center and CIAC in the USA, but it is good to note that also major vendors like SUN, Digital and Hewlett Packard are FIRST members.

FIRST, as noted above, is **not** involved in either the coordination or the actual handling of real incidents. This is done by the IRTs themselves. All IRTs have relations with a few fellow IRTs which they use to coordinate incidents. The only team assuming a "higher" responsibility in this scheme is CERT Coordination Center. They were installed in 1988 as the Internet IRT. This mission is increasingly difficult to maintain and may also invoke funding problems (current funding is by DARPA). But up until today, if an IRT doesn't have the right contacts to coordinate a specific incident, they hand it over to CERT Coordination Center or ask for their assistance. The majority of CERT Coordination Center's work is performed in working hours. Considering the timezone differences with the Pacific and European regions this causes a loss of efficiency when dealing with major international incidents.

1.6 European Status

In Europe there are currently nine FIRST members. Nordunet CERT, CERT-NL, DFN-CERT, JANET-CERT, RENATER-CERT, CERT-IT, and SWITCH-CERT are all research network IRTs. CCTA from the UK and BSI/GISA from Germany are government related teams. Several other networks in Europe are teaming up to become FIRST members (e. g. RCCN, CARNet, RedIRIS).

Considering the position of CERT Coordination Center described in the previous paragraph and the growing number of IRTs inside Europe it has been obvious since 1993 that some form of coordination between European IRTs other than bilateral should be organised, especially on behalf of incident coordination.

The final report of the RARE CERT Task Force (June 1994) pointed out this fact. The follow-up of this was the TERENA *ConCERT-in-E* proposal (November 1994). At the same time DANTE announced an *inCERT* coordination service for its customers IRTs. Neither of these initiatives has been successful to date. Next the TERENA Task Force „CERTs in Europe" was created in May 1995 to draw up a proposal for a way out of the current deadlock.

2 The Task Force Approach

The existence of a growing number of Incident Response Teams all over Europe is promising, though the coverage is by no means complete yet. The current ad hoc cooperation of existing teams is important but to solve the underlying problems and to meet the scalability demand a truly coordinated approach is crucial in the time to come. To address this need, various approaches can be taken, resulting in different levels of support and coordination. Initially the task force considered four different approaches. Three were considered viable options and are discussed in detail below. The fourth approach (Incident Handling) was dropped for the following reasons:

Incident Handling

In this approach a full incident handling capability would be provided. This would mainly address networks without their own Incident Response Team. As an additional service some support for new and existing teams could be offered. A coordinating role would not be a part of this service.

Due to the benefits and advantages of national or network based teams this approach was skipped for further analysis. It does not address the coordination issue nor does it prohibit duplications of effort due to new teams arising. In fact a centralised European Incident Response Team will face all of the same problems which are addressed by local teams – and more. It would be “just another CERT”, with little if no added value.

Three approaches remained for further analysis:

1. Incident Support
2. Basic Incident Coordination
3. Full Incident Coordination

The approaches were initially developed as separate entities. Soon it became obvious though that they really were three stages of the same model of European IRT coordination. This model offers a level of service which increases from Incident Support towards Full Incident Coordination. In every step services are added and the audience is widened.

2.1 Incident Support

This level of service provides a focal point for incident handling in Europe. It is intended to support existing teams, to help new teams and to promote incident handling and coordination. The latter should result in an increasing number of IRTs in European countries and networks.

The Incident Support level of service is abbreviated to IS in this section.

2.1.1 Services

Acting as a Focal Point for Europe

The most important aspect of this service is the provision of a focal point for Incident Response Teams. Both new and established teams in Europe will benefit from this. It will be the point where to ask for help and contact information of other teams. This focal point capacity will surely benefit successful incident handling in Europe and the world. A few examples now. When an incident involves sites in constituencies served by different teams, it is not always easy to find, authenticate and contact the appropriate IRT. IS will solve this problem by maintaining close relationships with the existing teams in Europe and providing the resulting contact information on its information server. This information would of course also benefit teams from other parts of the world, trying to contact an appropriate IRT but unfamiliar with any details of European networks. But probably the biggest help is envisaged when an incident involves sites that are in no team's constituency. It is expected that as a result of the promotion activities, there will be enough information on-line to also help cover these cases.

Note: this service is not intended to provide either incident handling or incident coordination, but solely to support IRTs in doing those jobs efficiently. Help in selecting and providing suitable contacts is an essential part of this support function.

Benefits: As described above, this service will help established IRTs and new teams to find appropriate contacts which is more and more difficult due to the growing number of European IRTs.

Promoting the Need for Incident Response Teams in Europe

In order to satisfy the security requirements in European computer networks, it is necessary to increase the number of IRTs at national and also organisational levels. The promotion service is therefore intended to encourage network service providers, organisations (academic and commercial) and other institutions to start their own IRTs. The promotion activities should be concentrated on those areas in Europe that are not being covered by any existing IRT. The following work-items are suggested:

- Identify trusted network and site contacts
- Increase awareness of network security problems and incidents
- Advertise the information server and other IS services
- Publish relevant articles, news, information about meetings and tutorials
- Other promotion activities

Benefits: Increasing the number of IRTs in Europe will not only benefit the European networks that will build those teams, but also the existing IRTs when dealing with incidents related to networks formerly not covered by any team.

Helping New Teams to Integrate into the European IRT Community

The main purpose of this service is to help organisations that are setting up their own Incident Response Teams. This should be done primarily through assistance in establishing contacts with existing IRTs which are willing to provide help. However, basic guidelines and recommendations for incident handling and forming an incident response team must be available on the information server. The service should also introduce new teams to the global community and help them to become FIRST members.

Benefits: The benefits of this service for new teams are the availability of basic guidelines and recommendations for their work and the assistance in integrating into the European and global IRT community. The proper setup and integration of new IRTs is itself a benefit for the established teams.

Establishing a Secure Communication Infrastructure

Secure (confidential and authenticated) communication between IRTs and their constituencies and between IRTs themselves is essential for successful incident handling. This service aims at enabling secure communication by providing the following functions:

- PGP key server
- Certification authority (CA):
  This CA will serve only IRTs in Europe. It will sign IRTs public keys for PEM (Privacy Enhanced Mail) and publish revocation lists. Later, it is expected to be integrated into the European CA infrastructure that will be developed in the near future within the CEU 4th Framework Programme projects.

This security infrastructure will also help to build up trusted relationships between teams since any new IRT will be properly authenticated before their keys are signed. Established policies on how certificates are issued, keys are signed etc. must be permanently available on the information server.

Benefits: European IRTs will be provided with a secure communication infrastructure that will enable authenticated and confidential communication.

Information Services

An information server should be set up in liaison with other IRTs and should contain any information relevant to prevention and handling of incidents (e. g. advisories, patches, tools, examples of site security policies). A crucial part of this information is an up-to-date and authenticated list of IRTs in Europe with their contact points and addresses. The information server will at least be composed of:

- WWW server
- Anonymous FTP server
- Mail based server

This service must also provide the maintenance of relevant mailing lists for the IRTs and possibly other interested parties.

Benefits: The main benefits of this service for established IRTs and new teams are an authenticated list of team contacts and mailing list for information exchange. Other information (e. g. tools, advisories, security policies) will help members of their constituencies and other users to increase the security of their systems and thus to prevent incidents.

Organising Meetings

Meetings and face-to-face discussions are essential for building trusted relationships between teams and exchanging experience. For that reason, one meeting/workshop per year will be organised co-located with other major events in Europe in order to reduce travel costs and also to enable contacts with experts in related areas. It is desirable that the meetings at least be attended by representatives of the European IRTs and by people from organisations that intend to start their own response team. IS will take care of the general organisation and minutes of the meetings. Host organisations must be found to enable the meetings and participants/organisations will cover their own expenses for attending.

Benefits: Meetings or workshops will help both new and established IRTs to exchange experience and build trusted relationships.

2.1.2 Target Set of Clients

- IRTs in Europe

- Organisations setting up their own IRT
- European Internet community

Not all clients are expected to be allowed to enjoy the same set of services. Trivially IRTs contributing to IS will enjoy all services, whereas the European Internet community will only have access to a subset of services.

2.1.3 Operation of Service

- Availability of information services:
  The information server must be available at all times. The operation of the other services in this model is less time critical and does not require permanent availability of the person in charge of this service.
- No incident handling or coordination.
- Contributing members:
  Contributing members will benefit from all available services and have direct access to IS staff. All others will only have access to the services publicly available through the information server.
- Cooperation and Liaisons:
  The IS staff is expected to be in close contact not only with IRTs in Europe but also with the main Incident Response and Coordination Teams outside Europe (like CERT Coordination Center) and associated bodies like FIRST, of which IS should be a liaison member. The staff is also expected to closely follow the work related to incident handling and security going on in relevant working groups of TERENA, IETF and ISO. Active participation in all groups is not required but dissemination of significant information emerging from these groups is. Finally, in order to avoid duplicate work within the IRT community, the IS staff should oversee and possibly initiate contacts between European IRTs and software or hardware vendors.

2.1.4 Resources

Staff:

- 1 FTE
- Level of experience:
  The staff responsible for this task represent a focal point for incident handling and coordination in Europe. Therefore, this staff must have not only secretarial and management skills but also technical ones as well as basic expertise in incident handling and an insight in incident coordination.

Equipment:

- Adequate network connectivity
- Workstation, printer etc.
- Access to information server with adequate diskspace
- Other communication equipment (phone, fax)

Offices:

- One office

Annual travelling:

- Intercontinental: 2
- Inter European: 3

To reduce the costs involved in setting up the Incident Support level of service and to save time in establishing trusted relationships, the IS staff could well be located within an existing, trusted and widely-known organisation. Good examples of such organisations are European IRTs that are also FIRST members, because they are accepted by the community, have understanding of the relevant tasks and have the necessary infrastructure elements already in place.

2.2 Basic Incident Coordination

This second level of service within the coordination model for European IRTs contains everything described in the Incident Support service level (see 2.1), but focuses on incident coordination as well. The daily routine of the incident handling process is still meant to take place in company or network IRTs, the coordination issue is one of interconnecting the right IRTs for a specific incident and constructing an overview of incidents and threats by functioning as an active focal point for IRTs.

The Basic Incident Coordination level of service is abbreviated to BIC in this section.

The main new items and topics of change are the following:

- Incident Coordination
- Round-the-clock available point of contact

- Real-time communication channel for IRTs
- Contacts with Incident Response and Coordination Teams outside Europe
- Extended information services
- Extended help for new teams

2.2.1 Services

BIC will provide all services outlined in 2.1.1, in some cases with added value. The extended and new services are outlined below.

Incident Coordination

BIC must have sound and trusted relationships with IRTs worldwide and in Europe specifically, know their operating procedures and have advertised its own in order to be able to perform incident coordination.

The need for coordination is caused by the wealth of IRTs from different networks and countries usually involved in serious incidents, with greatly varying knowledge of the global IRT community and equally varying skills in coordinating complex incidents. Therefore, an authoritative party (BIC), with specialised operational knowledge in the incident area, coordinating essentially global activities and efforts, often within small time-limits – is expected to be essential for successful, fast and consistent handling of incidents. The need for a European BIC will increase exponentially with the increasing number of hosts, sites, networks and IRTs in the European Internet community.

Next, BIC's ability to determine "patterns in crime" and thus reach conclusions faster than most IRTs, and their mission which implies always being up-to-date regarding the European and global situation concerning incidents and computer-crime, illustrates the value of such a European entity on a permanent basis.

Benefits: A significantly more effective handling of incidents on a European (and global) scale. The efficiency of this scheme rapidly increases with the growth of European networks.

Round-the-clock available Point of Contact

Because incidents have the world as a stage and different IRTs function in various time-zones, BIC should be available at all times for emergencies. All other business can be taken care of during normal working hours.

Benefits: Round-the-clock availability for BIC can substantially reduce the time needed to inform all parties involved in a threat or incident. This speed of operation will also be of great help when trying to prevent an actual threat from spreading further, by contacting IRTs and possible target-sites in a timely fashion.

Real-Time Communication Channel for IRTs

As the amount of networks and IRTs increases in Europe, there will also be an increasing need for BIC to act as a communication channel in order to initiate and maintain information flows between IRTs. For example:

- Small teams, network providers or sites will in some cases need introduction and authentication to non-European IRTs by a trusted party like BIC.
- Network users/providers or IRTs who don't know which European Team is appropriate to contact for an actual incident must be directed towards a responsible Incident Response Team. BIC can easily identify relevant parties and relay the necessary information.

The Incident Support service level also featured a communication channel function, but this was non-real-time and off-line. BIC's communication channel is real-time, because incident handling is real-time; and it is on-line, enabling BIC to assume its coordinating role at once when a specific incident would require doing so.

Benefits: Smooth set-up and flow of information between relevant parties, enabling IRTs to more concentrate on practical work, and enhancing the overview of BIC.

Contacts with Incident Response and Coordination Teams outside Europe

Not only must BIC entertain sound relations with European IRTs and network providers, but in order to effectively perform its duties it must also have fully trusted relationships with leading Incident Response and Coordination Teams outside Europe. This should be achieved by BIC's professionalism, effectiveness, confidentiality handling, availability and by being a contributing partner in incident related work. Joint meetings are an essential tool in establishing these relationships.

Benefits: Enhancement and enrichment of BIC's web of contacts. Crucial for efficient incident coordination, but also adding to the expertise of BIC staff and their shortlist of experts.

Extended Information Services

Information services, as described in 2.1.1, are a very important part of the BIC service. In addition to this information on the following topics should be provided:

- BIC's policy. By explaining the following aspects it should be made clear what BIC's function is, incident coordination rather than response:
  - BIC's mission
  - How to contact the team under what circumstances
  - How the team operates and performs its coordinating role
  - What level of confidentiality is to be expected
- Guidelines for establishing new IRTs.
- Early-warning and preventive information based on knowledge gathered in the coordination process and the monitoring of public security-related media.
- Pointers to legal information. Incidents involving multiple countries are subject to different national laws. BIC should gather and provide basic knowledge on how international computer crime is handled.
- Anonymised statistics of incidents in general and of BIC's proceedings specifically.

Benefits: Function and modus operandi of BIC are readily available. More extensive and ready-to-use information on computer security and incident handling is offered than inside the Incident Support service level.

Extended Help for New Teams

BIC will by design encourage the creation of new teams in Europe. As described in 2.1, providing information on "how-to" is one of the goals for BIC, but it should in addition actively monitor the creation process more closely and give guidance when necessary.

Benefits: As the IRTs are in a way BIC's primary tools, any properly established new team will contribute to the overall efficiency of incident handling.

2.2.2 Target Set of Clients

In addition to the set of clients mentioned in 2.1.2, since a mutual benefit is expected of the cooperation between the Basic Incident Coordination service level and Incident

Response or Coordination Teams outside Europe, the latter ones can also be regarded as part of BIC's target set of clients. More so than in the Incident Support case the subsets of BIC services available to different clients must be defined, since BIC has several potentially time-consuming services on offer.

2.2.3 Operation of Service

In addition to section 2.1.3:

- Availability:
  Since coordination of incidents is increasingly vital inside Europe's growing Internet community, the Basic Incident Coordination service must be reachable at all times.

  For the periods outside business hours, BIC should consider collaborating with an established IRT already featuring round-the-clock availability.
- No incident handling.
- Peer relationships:
  BIC must be a limited peer to other IRT coordination centers like specifically CERT Coordination Center. Limited peering means channeling relevant incident information to each other.
- Cooperation and liaisons:
  Apart from all bonds mentioned in 2.1.3 BIC must be a member of FIRST. This is essential for fully functioning in the international CERT environment.

2.2.4 Resources

Staff:

- 1 FTE – manager/administrative/technical
- 2 FTE – technical/administrative

Equipment:

- Adequate network connectivity, workstations, printers etc.
- File server with adequate diskspace for provision of information services
- Other communication equipment (phone, fax, cellular, pager)
- Router, terminal servers, modems, firewall to protect trusted information.

Offices:

- One office suitable for three persons

Travelling

- Intercontinental: 2
- Inter European: 5

Integration into an existing European IRT, already suggested for the Incident Support service level in section 2.1.4, will be equally useful for BIC.

2.3 Full Incident Coordination

Inside the coordination model for European CERTs described in this report, the Full Incident Coordination level of service provides the most comprehensive and active support when compared to the previously defined service levels. It is a natural successor to the Basic Incident Coordination service in an environment that will continue to grow in both size and demand.

The Full Incident Coordination level of service is abbreviated to FIC in this section.

The assistance offered to IRTs is significantly enriched in this highest level of service, and some new features are introduced. The main topics of change are the following:

- Extended incident coordination
- Non-stop support (24 hours a day – 7 days a week)
- Extended technical support (including vulnerability analysis)
- Educational role
- Emergency backup for teams

2.3.1 Services

FIC will provide all services mentioned in 2.2.1, in several cases with added value. The extended and new services are outlined below.

Extended Incident Coordination

FIC will provide the Incident Coordination service as outlined in 2.2.1. Due to the growth of the Internet in Europe this task will continue to grow in sheer size, i. e. quantity, but at the same time it is expected that the demand for quality will grow among FIC's clients. The latter is proposed to be tackled by guarding overall quality and by featuring a sound knowledge base and early warning system.

Because FIC will have data and information from the majority of IRTs and from FIRST, it is in a natural position to determine “patterns of crime”. FIC will maintain a database with structured information on attacks and vulnerabilities. Using this database FIC must issue early warnings on threats and vulnerabilities to relevant IRTs or networks. Also FIC should publish incident statistics, giving some measure of threat and success in meeting threat.

Benefits: FIC's coordinating role offloads IRTs in such a way that they can fully devote themselves to solving incidents, not having to worry about coordination issues. Duplication of effort is also minimised in this scheme. In addition to 2.2.1, FIC's knowledge base and early warning system will further enhance the effectiveness of its client IRTs and also be of use in helping to prevent threats from spreading rapidly, thus avoiding significant losses in time and money at end-user sites.

Non-Stop Support (24 Hours a Day – 7 Days a Week)

Exactly as described in 2.2.1 FIC should of course also be available at all times, but this time not only for emergencies but also for very serious problems. Additionally it is demanded that FIC be fully operational within half an hour after an incident has been reported outside working-hours. All business other than emergencies and very serious problems can still be taken care of during normal working hours.

Benefits: Like stated in 2.2.1, non-stop availability for FIC can substantially reduce the time needed to inform all parties (potentially) involved in a threat or incident. However, because of less constraints and a guaranteed response time, the FIC implementation will be more effective than its Basic Incident Coordination predecessor.

Extended technical support (including vulnerability analysis)

In the description of the Basic Incident Coordination service the offering of a limited degree of technical support is implicitly present, through the „communication channel“ and information server functions. FIC explicitly features technical support, meaning that advice will be given to client IRTs on how to deal with incidents and vulnerabilities. This advice must be of a practical but general nature. When FIC lacks specific knowledge, it is in a unique position to recruit this knowledge from elsewhere (client IRTs, CERT Coordination Center, vendors, R&D experts etc.).

Also FIC should actively audit existing and potential vulnerabilities and help find ways to fix or circumvent them. This must be done in close cooperation with vendors, other teams and individual experts. The results of this work should be made readily available.

Benefits: Sound technical support will help IRTs in doing their job properly. Eliminating vulnerabilities in applications and operating systems will prevent incidents from happening at all, thus saving considerable amounts of time and money.

Educational Role

FIC must organise and conduct educational awareness courses for the management of regional networks/providers. It should also educate technical staff of new and established IRTs in everyday tasks. Whenever possible courses will be combined with other events/meetings in order to minimise travelling costs for participants.

Furthermore, FIC should employ one "exchange pupil" from a client IRT. Purpose is to teach "in vivo" how to handle and coordinate incidents. Vice versa FIC can learn from the pupil's specific expertise. The pupil will work with FIC for a fixed period of time, e. g. 3 months, after which period a new pupil from another IRT will take his or her place. The expenses for the exchange pupil should be covered partially from FIC's funds and partially from the pupil's parent organisation.

Benefits: Successful awareness courses will help in creating a more solid base for IRTs to work on, with the management of companies and networks assuming the overall responsibility for security which is essentially theirs. Technical courses will help steepen the experience curve of client IRTs and thus enable them to more effectively handle incidents and coordinate with fellow IRTs and FIC.

Emergency Backup for Teams

FIC should serve as a backup for teams in cases of emergencies, when IRTs don't have round-the-clock support: FIC will then step in until the IRT takes over. The service provided in those cases is necessarily a bare minimum, the FIC lacking the detailed knowledge of IRTs' constituencies and lacking the humanpower to fully replace any IRT.

Benefits: Incident handling can begin even when the appropriate IRT is not yet available, therefore limiting damage.

2.3.2 Target Set of Clients

In addition to the points in section 2.1.2 and 2.2.2 FIC should restrict its extended technical and educational functions to contributing clients. It may prove useful to define different degrees of service which clients can subscribe to. This would reflect the great diversity among potential FIC clients, ranging from very small teams to IRTs with FIC's size or bigger.

2.3.3 Operation of Service

In addition to section 2.2.3:

- Availability:
  The Full Incident Coordination service must be reachable 24 hours a day, 7 days a week, and up-and-running within half an hour.
- Incident handling:
  Only bare-minimum incident handling on a temporary basis, until an appropriate IRT takes over.
- Peer relationships:
  FIC should be a full peer to other IRT coordination centers like specifically CERT Coordination Center. Full peering means channeling incident information to each other, sharing the bigger incident and threat picture and working together on open issues.
- Cooperation and liaisons:
  All bonds are already mentioned in 2.1.3 and the FIRST membership is postulated in 2.2.3.

2.3.4 Resources

Staff:

- 1 FTE – manager/technical
- 1 FTE – administrative/technical
- 3 FTE – technical

Equipment:

- Physically and logically separate network

- Workstations, printers, internal fileserver etc.
- Router, terminal servers, modems, firewall to protect trusted information.
- Adequate network connectivity
- External File server with adequate diskspace for provision of information services
- Other communication equipment (phone, fax, cellular, pager)

Offices:

- Two offices
- Resting room with bed

Travelling:

- Intercontinental: 3
- Inter European: 10

3 The Need for a Starting Point

Obviously the result of this task force's work is not the proposal of one or more single solutions to the coordination problems of IRTs in Europe and beyond. Instead of singular solutions a coordinating model is proposed which offers a migration path from a simple support function to a professional infrastructure for computer security incident handling within Europe. National and network oriented teams provide incident handling capabilities to their constituencies. The coordination of their work and international issues are addressed through incident handling coordination, which is to be supported at a European level. Given the enormous growth of the Internet, not least inside Europe, it seems unavoidable that the proposed migration path be generally followed: the simple Incident Support service will not suffice.

The task force's recommendation is to implement the Basic Incident Coordination service right away. While important parts of the Incident Support service are already being provided through the voluntary work of single teams the coordination issue can only be dealt with in a formalised and funded fashion, due to the resources necessary for this task.

To implement the Basic Incident Coordination service it is appropriate to first take over the Incident Support services scattered over the field. Therefore the task force recommends to start out with one FTE. The task of this person would be to learn from existing teams, take over the voluntarily provided services and add work-items and especially structure while doing so. After a short period (six to nine months) two FTE should be added to allow the setup of the team and – after additional education and training – to enable the team to become fully operational (nine to twelve months after starting out with one FTE).

It is further recommended to review the results of this service implementation after its first year of full operation, before deciding on how to progress towards Full Incident Coordination. This progress can be a gradual process. It is very importing (judging from actual experiences of existing teams) to allow at least one year of full operation before reviewing the success of the team (it will take a while to build up the necessary trust with all involved parties).

Regardless which approach is chosen by TERENA the build-up will benefit from the work of established teams and the existing and ongoing cooperation among European teams.

As today most existing European IRTs are mainly oriented towards national research networks it is natural to start the coordination activity within the European community of these networks. Due to the nature of the coordination task itself an isolated approach will not solve the underlying problems though, because incidents in all kinds of networks (research, private, commercial, banking industry, military, ...) must be coordinated. As this task will become more and more important in the future, reasonable steps should be taken to establish a flexible and enhanceable infrastructure which also allows the participation of other network communities later on.

This is comparable to similar approaches, where network wide services which are not limited to a specific community, are offered (like the services of the NCC). Although different teams exist in Europe it is much too early to expect a full infrastructure within the next years. It will take time to establish even only one Incident Response Team in every country, community or network. But with the need for it recognised and with a possible approach to help the parties involved in place, the most important action right now is to get things going and create a basis for this infrastructure.

4 How to proceed ...

4.1 Funding models

The European Coordination function is regarded as a **service** to the European CERTs and Incident Response Teams. Together with the decision on an initial service level made by TERENA GA, there must be a decision on the funding model.

Funding model examples:

A) Service:
European Coordination offers services which can be paid for by the customers, the „SURFnet model“.

B) Project:
European Coordination has a fixed budget given by funding from a central body, the „DFN-CERT model“.

B) Contributors:
The „NCC model“.

4.2 Proposed Time Schedule

The European Coordination should be introduced and start its work at the JENC 7 Conference in Budapest (T0). After this initial creation of the European Coordination function in the offices of the people doing the work, the level of activity will gradually be built up from one full time person equivalent (1 FTE) to three full time person equivalents (3 FTE) starting after six months (T0 + 6 months). By this time the team should start its full operation. After three months (T0 + 9 months), the office should be operational at the decided location with the specified number of FTE.

At T0+21 the project will be reviewed and the level of activity after T0+24 will be decided on.

Figure 4.2: Time Schedule

TO: JENC 7 – official starting point with 1 FTE

TO+6: taking over full operational status

TO+9: 3 FTE have taken over full operational status

TO+21: review process after first year of full operational status

TO+24: end of the first funding circle

4.3 Criteria for choice of Contractor and Office Location

The „Call for Tender“ procedure is regarded to be out of the scope of this Task Force. The recommended criterions for the selection of contractor and office location are given below.

- The contractor must be connected to an existing well-known CERT in Europe in the initial phase (T0 – T0+6). At T0+6 the additional person(s) (from any part of Europe) must be contracted to be a part of the team (TO+6 – TO+9).

- The final physical location of the office must be centralised at one (1) central location.
- The decision on physical location must be made by TERENA GA.
- Data encryption must be possible at the location.
- The office must be well connected to public transport facilities (international airport, local transport).
- The office must be connected to Internet with adequate capacity.
- The official language for the team is English.
- The office must be in a high level trusted technical environment. Co-location with an existing CERT may be useful.