Common Challenges Faced During the Establishment of a CSIRT

Dr Marthie Grobler
Defense, Peace, Safety and Security
Council for Scientific and Industrial Research
Pretoria, South Africa
mgrobler1@csir.co.za

Harri Bryk
CERT-FI
Finnish Communications Regulatory Authority
Helsinki, Finland
harri.bryk@gmail.com

Abstract— **A CSIRT is a team of dedicated information security specialists that prepares for and responds to information security incidents. When an incident occurs, members of a CSIRT can assist its constituency in determining what happened and what actions need to be taken to remedy the situation. The establishment of a CSIRT, however, is not without certain difficulties or complications. Such a project requires sustained commitment and relies largely on a circle of international trust that needs time to develop. Without these attributes, a CSIRT establishment project can run into a number of problems that can have varying effects on the successfulness of the project. This article looks at a number of common problems faced during the establishment of a CSIRT, within the set of chronological steps.**

Keywords-CSIRT, incident, establish, mandate, organization

I. INTRODUCTION

Communication networks and information systems have become an essential factor in economic and social development. Accordingly, the security of these networks and systems is of increasing concern to society. As a result, many national and international security communities started to collaborate for a more secure internet. These collaborations generally take the form of a CERT (Computer Emergency Response Team) or CSIRT (Computer Security Incident Response Team).

A CERT or CSIRT is a team of dedicated information security specialists that prepares for and responds to information security incidents. It is responsible for receiving, reviewing, coordinating and responding to computer security incidents and activities. When an incident occurs, members of a CSIRT can assist its constituency in determining what happened and what actions need to be taken to remedy the situation. This is especially important since communication networks and information systems have become an essential factor in economic and social development. Accordingly, the security of these networks and systems is of increasing concern to society.

II. BACKGROUND

CERT-FI, the Finnish national CSIRT, assisted South Africa in developing a capability for a national/coordinating CSIRT during the 2009/2010 financial year, spanning from March 2009 to March 2010. Due to unforeseen circumstances, the project was terminated prematurely. As a result, the project did not obtain all the planned objectives.

The purpose of this article is to share ideas on what to take into account when establishing a national/coordinating CSIRT or advising another country to establish a national/coordinating CSIRT. This article is based on the authors' own perceptions and does not necessarily reflect the opinions of the CSIR or CERT-FI. The following points and examples are not necessary all related to CERT-FI's development cooperation project in South Africa.

The next sections introduce a number of steps proposed to ensure the successful establishment of a national/coordinating CSIRT. These sections also briefly discuss common challenges identified during each of these steps. Figure 1 shows these steps.

Figure 1. Steps to follow during the establishment of a national/coordinating CSIRT

The steps mentioned in this article are adapted from the steps proposed by CERT/CC [1] and augmented by personal experience. For example, Step 1 – *Clarify mandate and policy issues,* is not normally a recommended step. However, based on the experience gained through the collaborative CSIR/CERT-FI project, this step is necessary for the future successful completion of a similar CSIRT establishment project.

III. STEP 1: CLARIFY MANDATE AND POLICY ISSUES

The first step in establishing a national/coordinating CSIRT relates to mandate and relevant policy applications. Usually, a

Acknowledgement must be given to the Council for Scientific and Industrial Research (CSIR) and the Finnish Communications Regulatory Authority (FICORA) for their financial support.

country in the process of establishing a national/coordinating CSIRT has some extent of involvement from the local government. This relates in particular to operations with national benefit. If the government is involved, there needs to be an appropriate and explicit mandate for any CSIRT establishing operations. Generally, if the mandate comes from the most senior position in government as far as possible, the better the chances to ensure a clear project mandate.

In several countries, many government departments have identified information security as one of their responsibilities [2]. Accordingly, openness and cooperation inside the government plays an important role when setting up a function like a national CSIRT. If possible, the team establishing the national/coordinating CSIRT needs to initiate and facilitate cross-sector conversations between different government departments. It might also be worthwhile to establish a working group or steering committee with actors from both government and private sector. This will not only widen the expertise but also commit other departments in the project even if their functions do not officially include information security.

Ambiguity or uncertainty with regard to mandate and responsibilities may lead to inefficient competition, delays in the project implementation and at worst, in termination of the project [3]. Other challenges in Step 1 relate to unclarity in mandate and inefficient competition.

In addition, it might sometimes be difficult to sort out the political playing field. The team establishing the national/ coordinating CSIRT should therefore try to contact other actors working in the same field in the target country to gain a big picture of current situation. Figure 2 presents the common challenges faced during the clarification of mandate and policy related issues.

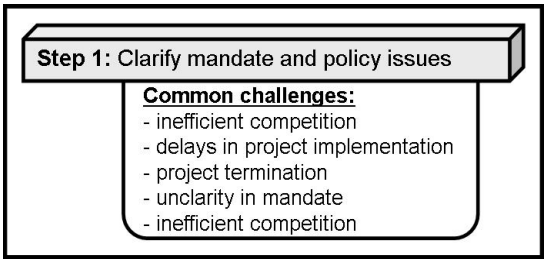

Figure 2. Common challenges faced during the clarification of mandate and policy related issues

At the latest when the CSIRT team is established and operational, it should have a proper mandate and the tasks should be defined in a legal source (act, decree or equivalent). This gives clarity and boundaries for the operations [2].

IV. Step 2: Obtain management support

The second step in establishing a national/coordinating CSIRT relates to obtaining senior management support within the organization trying to establish the CSIRT. In many instances, the individuals serving on the project team as well as intermediate managers are aware of the project and support it, whilst senior management might not necessarily be fully aware of the extent of the project, its implications and commitments, or have not explicitly given their support to the project team.

A key element for any successful project is to obtain management support within the organization driving the project. Management support should last throughout the project: from the planning to the implementation, through to the project closure [4]. In addition, it is important that management support be wide-ranging and displayed publicly in support of the project team.

Sometimes support itself is not enough and senior management should be able and willing to promote and drive the project. This is especially relevant when project problems occur. The team establishing the national/coordinating CSIRT should therefore ensure that senior management is behind the project and is willing to fight for it, before publicizing too much information about the project. Figure 3 presents the common challenges faced during the obtaining of management support.

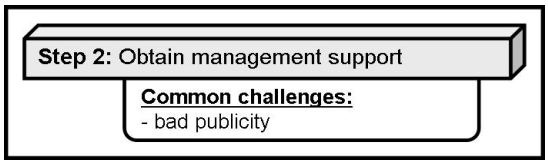

Figure 3. Common challenges faced during the obtaining of management support

Although publicity and the involvement of the information security community is an essential part of the development of such a project, it may cause severe public and reputation damage should senior management not support the project for its entire lifetime.

V. Step 3: Secure funding

The third step in establishing a national/coordinating CSIRT relates to securing financial support for the duration of the project. The team needs to ensure that there is enough funding for the entire project and that the funding can be allocated for the correct/required purposes. Changes to the original project plan and scope creep are common and therefore the funding should be flexible in that regard. The team should also reserve enough funding for contingency costs.

This step involves the creation of a well-defined annual budget that is separated into activities and functions. It will not only support the financial management process, but also help to recognize financial problems before they occur.

Once the cost related to an operational CSIRT has been considered, the CSIRT team needs to think about possible revenue models: how can the planned services be financed? The first option is the use of existing resources. The potential problem is that difficulties may arise in the organization itself regarding the distribution of resources between projects, e.g. non-CSIRT assignments are imposed by outside stakeholders that take staff away from their primary CSIRT functions and inhibit effective performance of normal services [6]. The second option is to sell CSIRT services to the constituency, with an annual/quarterly membership fee. Especially at the beginning of such a project, when the reputation of the CSIRT is not established, few people may be willing to pay for such services. The third option is subsidy provided from the government or a governmental body. The potential problem

regarding this option is political interference or mandate related problems.

The main challenge in this step is to find a source of investment to initiate the CSIRT establishment process. Figure 4 presents this challenge.

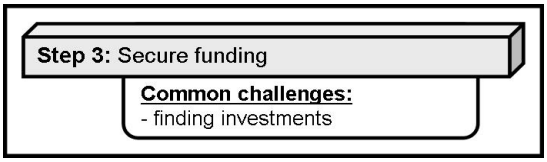

Figure 4. Common challenges faced during the securing of funding

The permanent funding might differ from the start-up funding. If the project has received separate start-up funding for the establishment phase, the project team needs to commence with negotiations for permanent funding at an early stage. The permanent funding should be available immediately after start-up without any interruptions.

VI. Step 4: Availability of Staff and Other Resources

The fourth step in establishing a national/coordinating CSIRT relates to the availability of project resources. Project staff is a crucial element for any project. In CSIRT activities professional expertise is crucial since people often do not have the necessary CSIRT skills before they are hired.

Usually new recruits undergo a thorough in-house-training of the needed CSIRT skills. Excellent IT-knowledge and willingness to learn new things are good characters in the recruiting process. In addition, there are good courses for learning basic CSIRT skills, such as the comprehensive CSIRT training course administered by TERENA TRANSITS [5].

In addition to human resources, technical resources also play a very important role in CSIRT operations. The team establishing the national/coordinating CSIRT should ensure that the team is able to purchase all needed equipment, accessories and systems - CSIRT operations rely heavily on specialized computer and IT equipment.

Sometimes a CSIRT's technical needs may conflict with the host organization's ICT policy and therefore it is beneficial to have a good standing relation with the host organization's IT department. If needed, the CSIRT team should produce its own ICT policies, and maintain and develop its own systems.

If the CSIRT team members' man-hours are separately listed in the budget, the person responsible needs to ensure that there is an appropriate monitoring system in place and that individuals do not exceed their allocated hours, inadvertently jeopardizing the future and continuation of the project. Figure 5 presents the common challenges faced during the securing of staff and other resources.

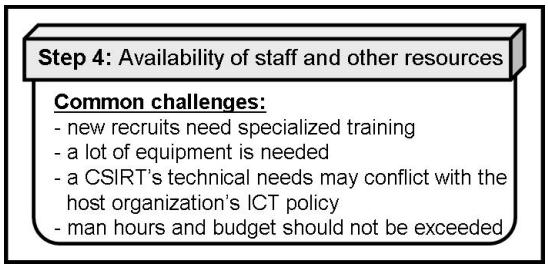

Figure 5. Common challenges faced during the securing of staff and other resources

VII. Step 5: Understand Cultural and Governmental Differences

The fifth step in establishing a national/coordinating CSIRT relates to cultural and working differences. This is especially relevant when there is a working relationship between two countries, where the one country advises on the establishment of a national/coordinating CSIRT in the other country.

Cultural backgrounds and working environments may differ greatly between different countries. Some of the potential problems relates to the cost and logistics of traveling between countries, decision-making and openness with regard to mandate and agendas, and political differences. For example, in the event of a negative decision, it is often hard to receive an answer that clarifies the problem. This is often the fault of bureaucracy, finding the right person or lack of gumption in decision-making, and obstacles relating to maintaining foreign relations.

This can generate unnecessary delays in projects and frustration among team members and stakeholders. At worst, stakeholders may lose trust in the organization hosting the CSIRT, potentially jeopardizing other/future projects with collaborators.

A lack of openness and understanding within the organization may also be a reason for slow decision-making. Colleagues are not aware of each other's ongoing tasks and in the case of absences, deputies cannot or are not allowed to take decisions on behalf of senior personnel.

In some organizations, traveling for business purposes is something unique and exclusive. Due to the international and networking nature of a CSIRT, team members may need to travel often. Unfortunately, traveling may bring about jealousy between employees of an organization.

This is problematic because in CSIRT activities with a national/coordinating function meeting people from key organizations is an important part of the operations. Figure 6 presents the common challenges faced with regard to cultural and governmental differences.

Figure 6. Common challenges faced with regard to cultural and governmental differences

VIII. STEP 6: THE BUSINESS PLAN

A business plan is a formal statement of a set of business goals, the reasons why they are believed attainable, and the plan for reaching those goals. The business plan is an important output from the business management approach to the CSIRT setting-up process. This step looks at the organizational structure and model, the services that will be provided by the CSIRT, staff and equipment needed.

The two main factors that influence the costs are the determination of service hours and the number of quality staff members to be used on the CSIRT project. At this stage of the project, it is necessary to consider whether a 24/7 incident response and technical support delivery is required, or whether the team will only be functional during office hours. Especially at the beginning of such a project, 24/7 shifts may be problematic for staff members accustomed to traditional office hours.

The suitable organizational structure of a CSIRT depends highly on the existing structure of the hosting organization and the constituency. It also depends on the accessibility of skilled experts to be hired permanently or on an ad hoc basis. A number of options are the independent business model, the embedded model, the voluntary model and the campus model. Each of these models has its own potential problems.

The equipment and utilization of office space and the physical security are very broad topics. Therefore, no exhausting description can be provided in this document. Since CSIRTs usually handle very sensitive information, it is good practice to let the team take control of the physical security of the office. This will depend very much on the existing facilities and infrastructure and the existing information security policy of the hosting company.

During this stage, it is also necessary for the CSIRT team to determine what services need to be offered to the CSIRT's constituency. A basic mistake when developing a business plan is to:

- offer too much services; the team should rather start small with limited team members and expand as necessary; and
- offer 24/7 service without a real need for it (constituents are not ready for this extended service).

Figure 7 presents the common challenges faced with regard to the business plan.

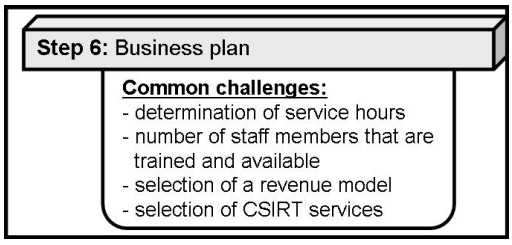

Figure 7. Common challenges faced with regard to the business plan

IX. STEP 7: TRAIN STAFF

Having decided on the services and the level of support to be delivered, the next step is to find the right amount of skilled people for the job. It is nearly impossible to provide hard figures on the amount of technical staff needed from this perspective, but the following key values have proven to be a good approach:

- deliver two core services of the distribution of advisory bulletins as well as incident handling: a minimum of four full time employees (it is important that the team focus on the incident handling services in order to be called a CSIRT).
- full service CSIRT during office hours, and maintaining systems: a minimum of six to eight full time employees.
- fully staffed 24/7 shift (two shifts during out-of-office hours), the minimum is about twelve full time employees [7].

These numbers include redundancies to provide for sick leave and vacation leave, etc. It is necessary to check the local labor agreements - if people work outside office hours this might result in extra costs in the form of extra allowance that have to be paid.

To build a CSIRT with capable incident handlers, people with a certain set of skills and technical expertise are needed, as well as abilities that enable them to respond to incidents, perform analysis tasks, and communicate effectively with your constituency and other external contacts. These people must be competent problem solvers, must easily adapt to change and must be effective in their daily activities [8][9].

It is often not easy to find such qualified staff, so sometimes CSIRTs nurture and train internal staff members to advance into these incident-handling roles. This can be an expensive, time-consuming process. There is always the risk that trained key personnel may resign and leave the CSIRT. Staff is often not cross-trained, where a single individual is responsible for a specific function [6]. Figure 8 presents the common challenges faced with regard to training staff.

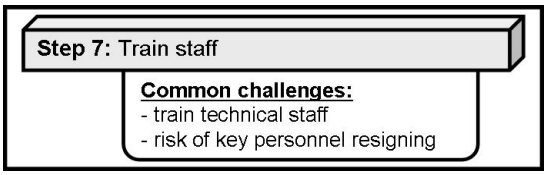

Figure 8. Common challenges faced with regard to training staff

X. STEP 8: DEVELOP OPERATIONAL AND TECHNICAL PROCEDURES

Operational and technical procedures are a particular course of action prescribed by the specific entity, to ensure an intended result. Operational and technical procedures and policies are necessary to ensure that the CSIRT members handle incidents in a consistent way. The process of information handling during incident handling is very similar to that used during the compilation of alerts, warnings and announcements.

The information gathering part usually is different, as the normal way to get incident related data is either by receiving incident reports from the constituency or other teams, or by receiving feedback from involved parties during the incident handling process. Information usually flows by (encrypted) e-mail; sometimes the use of telephone or fax is necessary.

The potential challenges are that the CSIRT is not yet operational at this stage. This may lead to an incorrect understanding of processes, potentially leading to incorrect operational and technical procedures. In addition, the team establishing the national/coordinating CSIRT cannot test the procedures with valid incidents, rendering the procedures potentially invalid in real-life incidents. Figure 9 presents the common challenges faced with regard to operational and technical procedures.

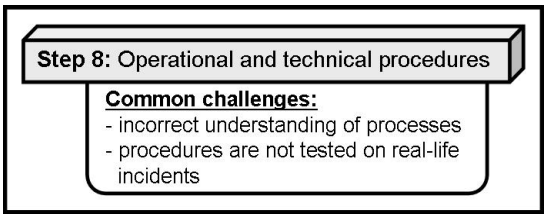

Figure 9. Common challenges faced with regard to operational and technical procedures

The development of the operational and technical procedures is a very crucial stage in the establishment of a national/coordinating CSIRT. Therefore, the success of the operational CSIRT will depend strongly on the quality of the technical and operational procedures. This step also relies heavily on policies and best practices relevant to incident response teams.

XI. STEP 9: MAKE THE CSIRT OPERATIONAL

Once the CSIRT is properly set up, the CSIRT team should ask the host organization's management to make a formal announcement, both to the existing constituency as well as the general public. This step includes the distribution of marketing material and incident reporting guidelines explaining how the constituency should interact with the CSIRT [6].

At this stage, the CSIRT team should also concentrate on ways to disseminate information about the CSIRT services, such as intranets, web sites, brochures, seminars and training classes. The most common problem that may occur during this step is that the CSIRT is not formally announced, and no one understands how or when to interface with the team [6]. Figure 10 presents the common challenges faced with regard to making the CSIRT operational.

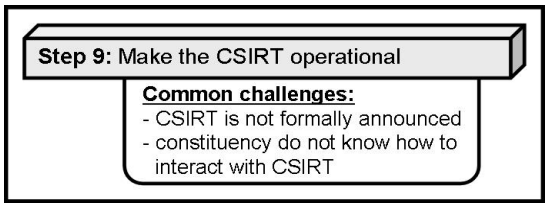

Figure 10. Common challenges faced with regard to making the CSIRT operational

XII. DISCUSSION

Table 1 shows a summary of the proposed steps and associated challenges identified through this article.

TABLE I. CSIRT STEPS AND ASSOCIATED CHALLENGES

Proposed step	Identified challenges
1 – Clarify mandate and policy issues	– inefficient competition – delays in project implementation – project termination – unclarity in mandate – inefficient competition
2 – Obtain management support	– bad publicity
3 – Secure funding	– man hours and budget should not be exceeded
4 – Availability of staff and other resources	– new recruits need specialized training – a lot of equipment is needed – a CSIRT's technical needs may be against the host organization's ICT policy
5 – Understand cultural/ governmental differences	– costs and logistics of travelling – slow decision-making – lack of openness – political differences – maintaining foreign relations – bureaucracy – unnecessary delays – lost stakeholder trust
6 – The business plan	– determination of service hours – number of staff members that are trained and available – selection of a revenue model – selection of CSIRT services
7 – Train staff	– train technical staff – risk of key personnel resigning
8 – Operational and technical procedures	– incorrect understanding of processes – procedures are not tested on real-life incidents
9 – Make the CSIRT operational	– CSIRT is not fully announced – constituency do not know how to interact with CSIRT

Table 1 does not provide an exhaustive list of challenges that can be faced during the establishment of a CSIRT. These proposed steps are based on the authors' own perceptions and experiences, within the context of one country advising and

mentoring another country in establishing a national/ coordinating CSIRT. Other challenges that can also be faced during the establishment of a CSIRT relates to business and risk management, internal auditing and information security.

XIII. CONCLUSION

In conclusion, this article shared ideas on what to take into account when establishing a national/coordinating CSIRT or advising another country to establish a national/coordinating CSIRT. The challenges faced during such a project depend on the countries involved, the individual team members working on the project, as well as a number of external factors. Thus, each project may face its own combination of unique challenges.

The value of this article lies in the practical hands-on guidance on what to do and what not to do during such a project. Although the paper is intended for the establishment of a CSIRT on national level, all of the steps and most of the challenges are also relevant when establishing a sector-specific or organizational CSIRT.

REFERENCES

[1] Killcrece, G. 2004. Steps for Creating National CSIRTs. Software Engineering Institute, Carnegie Mellon University, URL: http://www.cert.org/archive/pdf/NationalCSIRTs.pdf (Accessed 12 April 2010).

[2] Bryk H. 2008. A study among certain European computer security incident response teams and application of good practices in Finnish Communication Regulatory Authority', Helsinki University of Technology, Espoo, Finland. December 2008, 84 p. (in Finnish)

[3] CERT-FI. 2009. National and Governmental CSIRTs in Europe. URL: http://www.cert.fi/attachments/certtiedostot/5kiBC9Qy0/National_and_ Governmental_CSIRTs_in_Europe.pdf

[4] ENISA. 2008. A basic collection of good practises for running a CSIRT. URL: http://www.enisa.europa.eu/act/cert/support/guide2/files/ a-collection-of-good-practice-for-cert-quality-assurance/at_download/fullReport

[5] TERENA. 2010. CSIRT training. URL: http://www.terena.org/ activities/csirt-training/ (Accessed 6 April 2010).

[6] CERT/CC. 2006. Action List for Developing a Computer Security Incident Response Team (CSIRT). URL: http://www.cert.org/ csirts/action_list.html (Accessed 2 March 2010).

[7] ENISA. 2007. A step-by-step approach on how to set up a CSIRT. URL: http://www.enisa.europa.eu/act/cert/ support/guide (Accessed 29 October 2009).

[8] Killcrece G, Kossakowski KP, Ruefle R & Zajicek M. 2003. State of the Practice of Computer Security Incident Response Teams (CSIRTs). Software Engineering Institute, Carnegie Mellon University. URL: www.cert.org/archive/pdf/03tr001.pdf (Accessed 12 April 2010).

[9] West-Brown MJ, Stikvoort, D, Kossakowski KP, Killcrece G, Ruefle R & Zajicek M. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs). Software Engineering Institute, Carnegie Mellon University. URL: www.cert.org/archive/pdf/csirt-handbook.pdf (Accessed 12 April 2010).