# **Managing CSIRTs** [Computer Security Incident Response Team]

### *Introduction: What is a CSIRT?*[1]

Computer networks have become a backbone of any modern business enterprise; they not only facilitate regular business activities, but frequently are central in gaining competitive advantage. At the same time, computer-based information technology has introduced a new and substantial risk to business operations.

Many remember the turmoil and anxiety sparked by the Y2K (Year 2000) problem. Countless publications discussed doom scenarios that could occur given a failure of critical parts of the computer-network infrastructure; costs of recovery from the computer-network downtime were also high on the discussion agenda. While the Y2K challenge was tackled successfully, the lesson was clear: computer information infrastructure is critical for the performance of any modern organization.

Currently, the main threats to the reliability of computer infrastructure are intrusions and malicious attacks by external or internal actors. Most organizations appreciate the need for ensuring the security of their computer networks. Still, even the best IT-security infrastructure cannot guarantee that intrusions and malicious acts will not happen. The resulting damage and recovery costs will depend on the organization's ability to recognize, analyze, and respond to an incident.

A CSIRT – Computer Security Incident Response Team – is a service organization established to assist business or government organizations in handling computer security incidents. A typical CSIRT is responsible for receiving, reviewing, and responding to computer security incident reports. It may also provide a range of proactive services, including issuing early alerts to potential problems or conducting IT-security staff trainings.

CSIRTs range from on-site internal units, which service one particular organization, to national coordination centers, which provide incident handling services to an entire country or region. Most of the CSIRTs do not charge direct fees for their services. Rather, they are funded by their constituency/parent organization (a commercial or government entity) depending on the scope and number of provided services. Development of new services and maintenance of the existing services is therefore crucial to the survival and growth of any CSIRT. However, such growth must be carried out with care. To understand why, it is useful to introduce the concept of '*CSIRT capacity*'.

[1] Based on information published at http://www.cert.org/csirts/ (accessed February 11, 2005)

### *CSIRT capacity and its service level*

CSIRT capacity may be thought of as the ability of the team to provide computer incident related services: the greater the capacity, the greater the challenges that can be handled by the team.

The capacity may be expressed as the total number of average person-hours that a CSIRT is capable of delivering during one hour. The contribution of the individual staff members will vary depending on their proficiency to carry out the tasks. More experienced staff will be able to perform the tasks quicker, thus contributing more capacity than a less experienced or knowledgeable team member.

CSIRT capacity expressed in terms of average person-hours is further elucidated in Figure 1. Both CSIRTs depicted in Figure 1 consist of 5 staff members. Despite the same level of staffing, each team has a different overall capacity. This is due to the difference in the levels of expertise of the staff on each team.

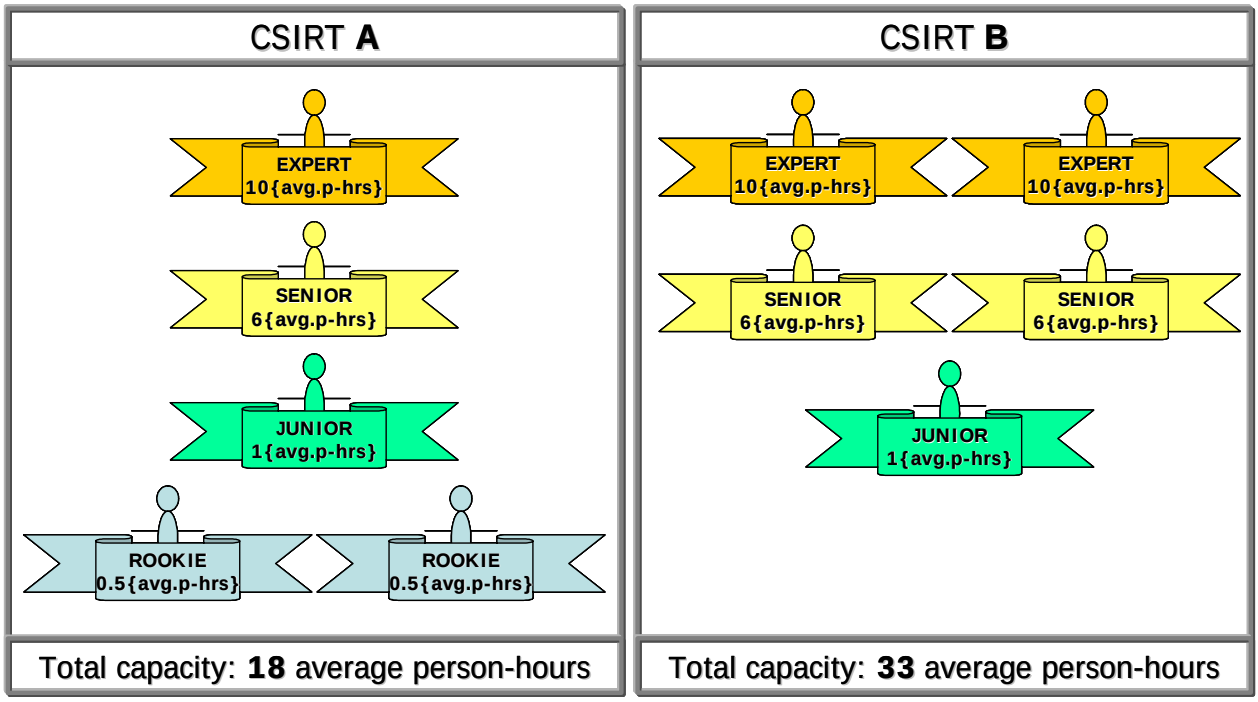



**Figure 1** Conceptual illustration of the CSIRT capacity estimation.

The greater the CSIRT capacity, the higher the number of services that can be provided by the CSIRT. However, one should be aware that providing services depletes the overall capacity. This occurs because incident handling is stressful and causes fatigue, decreasing the ability of the staff to respond effectively; consequently, the CSIRT capacity is reduced. The capacity is regenerated when the staff is involved in research, training or software development – these activities are "non-stressful," often creative and exciting. Note that they not only help to reenergize the staff but also prevent the staff's skills and knowledge from becoming obsolete. They may also lead to an increase in the team's capacity (e.g., when new expertise is developed or new tools that allow for more effective incident handling are produced).

These capacity-enhancement activities are indispensable for the survival of any CSIRT; they are the only way to regenerate the capacity that is depleted when providing the services. Moreover, they allow the CSIRT to replace capacity that becomes obsolete or to increase capacity through acquisition of new capabilities. However, one should not forget that these capacity-enhancement activities also utilize some of the existing CSIRT capacity. Therefore care should be taken for the capacity not to be depleted completely by excessive service volume. (Given no capacity, the team will neither be able to provide services nor enhance its capacity.)

Achieving an appropriate and sustainable service level is one of the main challenges faced by CSIRT managers. A sustainable service level means providing the highest possible number of services (ensuring the highest possible funding) while maintaining the CSIRT capacity in the long-run – i.e., the CSIRT is able to restore all the capacity that is depleted when providing services.

In this challenge you will be asked to play the role of a CSIRT manager and to restore a sustainable service level for your team. Detailed instructions for carrying out this task follow.

***INSTRUCTIONS***

You will play the role of the CSIRT manager. Your funding depends on the number of services provided by your team. Your main objective is to provide as wide a range of IT-security services as possible. Note, however, you should make sure that your operation is sustainable. This means that you should aim for the highest possible sustainable service level.[2] You should also try to reach this desired state as quickly as possible.

The only decision you will make is to set the number of services that will be provided by your team during the next decision period. You make your decisions quarterly for 4 years, i.e. you have 16 decisions to reach the desired state. You will have 3 trials. However, do the best you can in each of them. The participant who gets the best results (i.e., reaches the sustainable service level quickest) will receive a symbolic prize.

You are managing a fixed size CSIRT team that is the only entity of this type operating in your region – i.e., you are not competing with anybody else for constituency support. The primary goal of any CSIRT is to assist its constituency/parent organization. The limiting factor in providing the services is the CSIRT capacity to handle and prevent security incidents.[3]

The net growth of the CSIRT capacity depends on the current capacity level:

- When the CSIRT capacity is low, its net growth will also be low due to insufficient support available for capacity-enhancement activities.
- With high CSIRT capacity levels, the net capacity growth again tends to zero: the only development occurring will concern update and upgrade activities.

In between these extremes, the net CSIRT capacity growth reaches its maximum.

The CSIRT operations may be further characterized by the following piece of information:

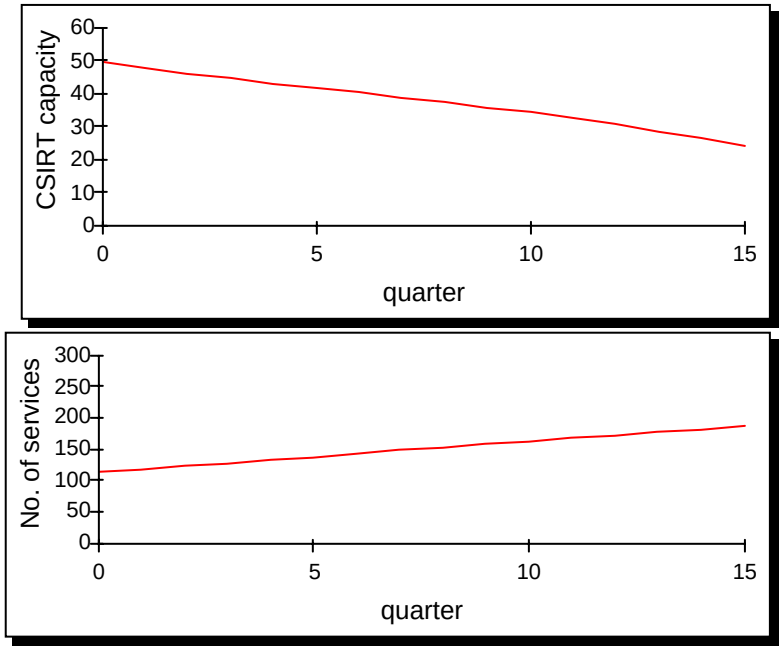
- In one quarter, providing 100 services reduces the CSIRT capacity level by 4 average person-hours. We simplify and assume that the capacity loss estimate is uniform for all services and is independent of the CSIRT capacity level: as long as the CSIRT has any capacity, services are provided (e.g., given the capacity level of 2 average person-hours, the CSIRT will be able to provide only 50 services in the quarter).
- For the purpose of this task you can vary freely the number of services provided by your CSIRT: You can increase or decrease its size arbitrarily at any point in time. The changes will be in effect immediately for the next decision period and will not affect the future funding in any way (i.e., even if you cease providing services for the constituency, the funding will be restored automatically as soon as the services are reestablished).

[2] See p. 3 for definition of sustainable service level
[3] See p. 3 for details

All data regarding the number of services provided by your CSIRT and the CSIRT capacity level are “perfect” (no “noise”, no “distortions”) and there are no random variations in between the decision periods in the service number or the growth of the CSIRT capacity.

Before you take over your CSIRT, you need to know that the previous manager has increased steadily the number of services provided from 115 to 185 over the past 4 years. As a consequence, the CSIRT capacity [average person-hours] has dropped from the initial 50 average person-hours to 24.4 average person-hours at present. This development is shown in the diagrams and table below.

**Historical development**




| CSIRT capacity | No. of services |
|---|---|
| 50.0 | 115 |
| 48.2 | 120 |
| 46.5 | 125 |
| 45.0 | 130 |
| 43.6 | 135 |
| 42.1 | 140 |
| 40.7 | 145 |
| 39.3 | 150 |
| 37.8 | 155 |
| 36.3 | 160 |
| 34.7 | 165 |
| 32.9 | 170 |
| 31.1 | 175 |
| 29.1 | 180 |
| 26.9 | 185 |
| 24.4 | *Your 1st decision* |