A Generic National Framework For Critical Information Infrastructure Protection (CIIP)

Manuel Suter, Center for Security Studies, ETH Zurich

August 2007

August 2007

International Telecommunication Union

Acknowledgements

This research paper, entitled *A Generic National Framework for Critical Information Infrastructure Protection*, was commissioned by the ITU Corporate Strategy Division (CSD) and the ITU Bureau for Telecommunication Development's ICT Applications and Cybersecurity Division (CYB). This paper aims to outline a possible simple framework that could be of interest to developing countries which desire to establish a national Critical Information Infrastructure Protection (CIIP) programme. The framework is modeled after the Swiss Reporting and Analysis Center for Information Assurance (MELANI). The author, Manuel Suter, is from the Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zurich, Switzerland, which produces the *International CIIP Handbook: An Inventory and Analysis of National Protection Policies*.

The Center for Security Studies has previously produced the study, *A Comparative Analysis of Cybersecurity Initiatives Worldwide*.

The views expressed in this paper are those of the author and do not necessarily reflect the opinions of the ITU or of its membership.

This paper has been submitted to ITU-D Study Group Question 22/1: *Question 22/1: Securing information and communication networks: best practices for developing a culture of cybersecurity* for their consideration.

Abbreviations

CCB	Closed customer base
CERT	Computer Emergency Response Team
CI	Critical infrastructures
CII	Critical information infrastructures
CIIP	Critical information infrastructure protection
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response and Security Teams
ICT	Information and Communication Technology
ISAC	Information Sharing and Analysis Center
IT	Information Technology
ITU	International Telecommunication Union
ITAA	Information Technology Association of America
MELANI	Melde- und Analysestelle Informationssicherung (Reporting and Analysis Center for Information Assurance)
OCB	Open customer base
PCCIP	Presidential Commission on Critical Infrastructure Protection
PPP	Public-Private Partnership
SME	Small and Medium-sized Enterprise
WARP	Warning Advice and Reporting Point

Table of Contents

1 INTRODUCTION: WHY A GENERIC NATIONAL FRAMEWORK?

Societies all over the world are becoming more highly dependent on information technology. Critical Information Infrastructure Protection (CIIP) is universally acknowledged as a vital component of national security policy. In order to protect their critical infrastructure, some countries (in particular, the Western European and North American states) have established sophisticated and comprehensive CIIP organizations and systems, involving governmental agencies from different ministries, with a variety of initiatives. These programmes try to cover all the different facets of CIIP, ranging from reducing vulnerabilities and fighting computer crime to defense against cyber-terrorism. However, due to their complexity and country context, these CIIP models are not necessarily applicable to other countries. Furthermore, many existing solutions are fairly resource-intensive and therefore not suitable for the majority of countries in the world.

For states that are starting to develop their own CIIP policy, it is often difficult to identify best practices and good examples. Many of these states may not have the same resources as the industrialized nations and cannot build complex and comprehensive organizations; rather, they can only focus on implementing only the most urgent measures. This paper provides a generic framework in order to help these countries to determine their response to the challenges of CIIP. It draws on different existing CIIP models, in particular, the Swiss CIIP model, to suggest a functional model for a CIIP unit that can promote collaboration between existing stakeholders to protect the state's critical infrastructure and services. Over the last couple of years, the Swiss Reporting and Analysis Center for Information Assurance (MELANI)[1] has proved a good example of a small, but effective CIIP organization.

The generic model for CIIP presented here is not a cure-all; instead, this paper offers a few building-blocks for a functional CIIP unit. By concentrating on top priorities, cooperation between various stakeholders, flexibility and adaptability, relatively inexpensive solutions can be developed to meet country-specific needs. As the structure of the CIIP unit has to be designed in relation to its essential tasks, identifying the main duties and responsibilities is vital. Thus, the paper starts by describing the essential tasks of CIIP. In section 3, the cooperation model is introduced. Since CIIP units have to deal with tasks that are highly diverse, strong partners are needed. The paper examines which partner should be responsible for which task. A potential organization chart for CIIP units is presented in section 4, and the responsibilities for national and international networking (which is vital for an effective CIIP unit) are discussed in section 5. Section 6 discusses the different customers that the CIIP unit should serve. Finally, a case study illustrates how a CIIP unit designed according to this framework could work in practice.

2 ESSENTIAL TASKS: THE FOUR PILLARS OF CIIP

Considering the variety of tasks affiliated with CIIP, the first step towards an effective and efficient CIIP organizational unit is to define its essential priorities and responsibilities. These essential tasks of CIIP are arranged in a "Four-Pillar Model" of CIIP. The four pillars of this model are: prevention and early warning; detection; reaction; and crisis management. This section describes the four pillars and defines which role the CIIP organization should play in each of these four pillars.

2.1 Prevention and Early Warning

Prevention and early warning are indispensable components of CIIP. They aim to reduce the number of information security breaches. However, since threats to CIIP are manifold, interdependent, and complex, it is unrealistic to expect that incidents can be altogether prevented.[2] A more realistic goal is to ensure that critical infrastructures "are less vulnerable to disruptions, any impairment is short in duration and limited in

[1] http://www.melani.admin.ch/index.html?lang=en

[2] Holderegger, Thomas (2006): The Aspect of Early Warning in Critical Information Infrastructure Protection (CIIP), in: Dunn, Myriam and Victor Mauer (eds.): International CIIP Handbook 2006 Vol. II: Analyzing Issues, Challenges, and Prospects (Zurich: Center for Security Studies), p. 112.

scale, and services are readily restored when disruptions occur."[3] The main function of prevention is to ensure that companies operating critical infrastructures are prepared to cope with incidents.

In one way or another, all pillars of CIIP contain elements of prevention (e.g., an adequate and effective reaction may deter attackers and may thus also include preventive characteristics). In this paper, prevention is defined in the narrow sense as consisting of activities that raise the general preparedness of companies. This involves the dissemination of recommendations and guidelines on best practices, timely and credible warning of specific threats, and the implementation of training and exercises. It is worth noting that prevention and early warning cannot be approached on a purely technical level - potential dangers have to be weighed up constantly in a trade-off against risk situations.

The CIIP unit discussed by this paper should promote prevention measures, by hosting workshops in which protection measures and best practices are discussed, as well as disseminating warnings and advice. However, although these tasks are essential, the CIIP unit is not the only source of support and guidance in information security. The operators of CII know their business better than most governmental units and there are other sources of warnings and advice. Therefore, the CIIP unit should focus its services on types of support that are not readily available elsewhere. In consequence, the workshops, warnings, and advisories should be tailored to the specific needs of operators of CI, with exclusive information.

The CIIP unit can provide exclusive information because it is in an exceptional position. As a government body, it may be perceived as neutral and free from commercial interests. Its workshops, warnings and advice may be seen as more credible than the products of private information security consultants. In addition, a well-designed CIIP unit has a large network of contacts at its disposal, with access to exclusive information. The CIIP unit can foster information-sharing among companies and raise their awareness of their interdependency. In this respect, it can act as a neutral and safe platform where experiences and knowledge can be shared among the different operators of CI.[4]

The task of prevention with regard to the operators of CI can therefore be accomplished selectively and without incurring immense operating expenses. Apart from this, however, new forms of attacks (e.g. Distributed Denial of Service (DDoS) attacks[5]) involve the use of huge numbers of compromised computers to attack systems, showing that prevention measures should not be limited solely to the operators of CI. Every connected computer that is not sufficiently protected threatens the security of all other connected systems. The CIIP unit has to focus also on prevention measures for the benefit of the broader public. However, since this task is time-consuming and cost-intensive, the CIIP unit needs supporting partners. Supporting partners may be found in private-sector associations (e.g., industry associations), among IT manufacturers and software producers, among other governmental organizations (e.g., data protection agencies), in the academia or in the media. Preventive measures aimed at the broader public are only successful when they are supported by different actors; they cannot, and should not, be accomplished by the CIIP unit alone.

2.2 Detection

Detection is the second pillar. In order to promote security and to avoid particularly vulnerable technologies, it is crucial that new threats be discovered as quickly as possible. In order to recognize emerging threats on a timely basis, the CIIP unit depends on a broad national and international network. In close collaboration with technical experts from Computer Emergency and Response Teams (CERTs),[6] the CIIP unit should identify new technical forms of attacks as soon as possible. Furthermore, non-technical analyses of the general risk situation are needed (e.g., information about the emergence of criminal organizations). Thus, the CIIP unit should have restricted access to certain relevant information provided by intelligence services. In addition, technical as well as non-technical information may need to be shared with international partners, since the threats to information security are not limited to geographic borders.

---

[3] Juster Kenneth I. and John S. Tritak (2002): Critical Infrastructure Assurance: A Conceptual Overview, in: Joint Economic Committee, United States Congress: Security in the Information Age – New Challenges, New Strategies (Washington, DC: White House), p. 12.

[4] For a more detailed discussion on information-sharing with and within the private sector, see Section 6.1.3.

[5] For a definition of DDoS attacks, see: http://en.wikipedia.org/wiki/Ddos#Distributed_attack.

[6] The cooperation with CERTs is described in Section 3.2.

However, the network of contacts belonging to CERTs and the intelligence services is of only limited use without the close cooperation of the operators of CI. After all, CI operators are affected first and foremost by new attacks, and if they fail to report incidents, detection and early warning become impossible. The importance of information-sharing with and within the private sector was highlighted in the US federal government's 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP).[7] Nevertheless, information-sharing is generally still only limited and many initiatives for information-sharing have proved only partly successful.[8] This is mainly due to the fact that companies share information only under conditions of strictest confidence. Building trust is a major task for any CIIP unit, in order to obtain information about incidents directly from the firms. How these demanding tasks can be achieved is discussed further below.

2.3 Reaction

Reaction includes the identification and correction of the causes of a disruption. Initially, the CIIP unit should provide technical help, and support to the targeted company. However, the CIIP unit cannot take on the management of incident response for these companies. The activities of the CIIP unit should complement, but not replace, the efforts of companies. Instead, the CIIP unit usually provides advice and guidance on how to tackle an incident, rather than offering complete solutions.

A major requirement for accomplishing this task is that the CIIP unit must have a 24/7 incident reporting service. Attackers often prefer to execute their attacks on the information infrastructure of companies at times when they expect to face few immediate countermeasures. To a large extent, the damage caused by an attack depends on how long it takes to stop it. Therefore, incident response must start as quickly as possible. The support provided by the CIIP unit is most helpful, if it is always available.

However, similar to prevention and detection, incident response is not restricted to technical measures. In particular, prosecution of attackers is a vital part of reaction. Law enforcement may not be able to help targets directly, but it can help protect others by increasing the risk of capture, prosecution and wider deterrent.[9] Since many attacks are carried out by international actors, companies often do not know how to secure appropriate law enforcement responses abroad. The CIIP unit should support targeted companies by referring them to the responsible authorities.

Finally, adequate reaction also includes analysis of incidents. In cooperation with the target, the CIIP unit should draw up a final report on the incident. The lessons learned should be made available to other operators of CI. The private industry tends to focus mainly on lessons learned to improve their internal systems, but the government can take a somewhat broader approach. Lessons learned should be exchanged with all critical players in order improve crisis planning and to streamline information-sharing in crisis situations. Companies and government sectors that were not affected by the attack can compare emergency plans and take steps to avoid mistakes. This concludes the cycle of prevention, detection, reaction, and crisis management.

2.4 Crisis Management

Crisis management has been part of CIIP since its inception. Minimizing the effects of any disruptions on society and the state has always been a major task of protection, so the CIIP unit must be embedded in the national crisis management structure. Depending on the organization of a state's crisis management administration, the CIIP unit can be positioned in several different ways. It should be well-positioned in order to have direct access to decision-makers, because a key function of the CIIP unit is to alert the responsible people and organizations. In case of a national crisis, the CIIP unit must be able to offer advice directly to the government.

---

[7] United States Government Accountability Office (GAO) (2004): Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors (Washington, DC: White House), p. 8.

[8] Poulsen, Kevin (2005): U.S. Info-sharing Called a Flop, in Security Focus, 11 February 2005. Available at: http://www.securityfocus.com/news/10481.

[9] Schechter, Stuart E. and Michael D. Smith (2004): How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks (Cambridge, Cambridge University Press).

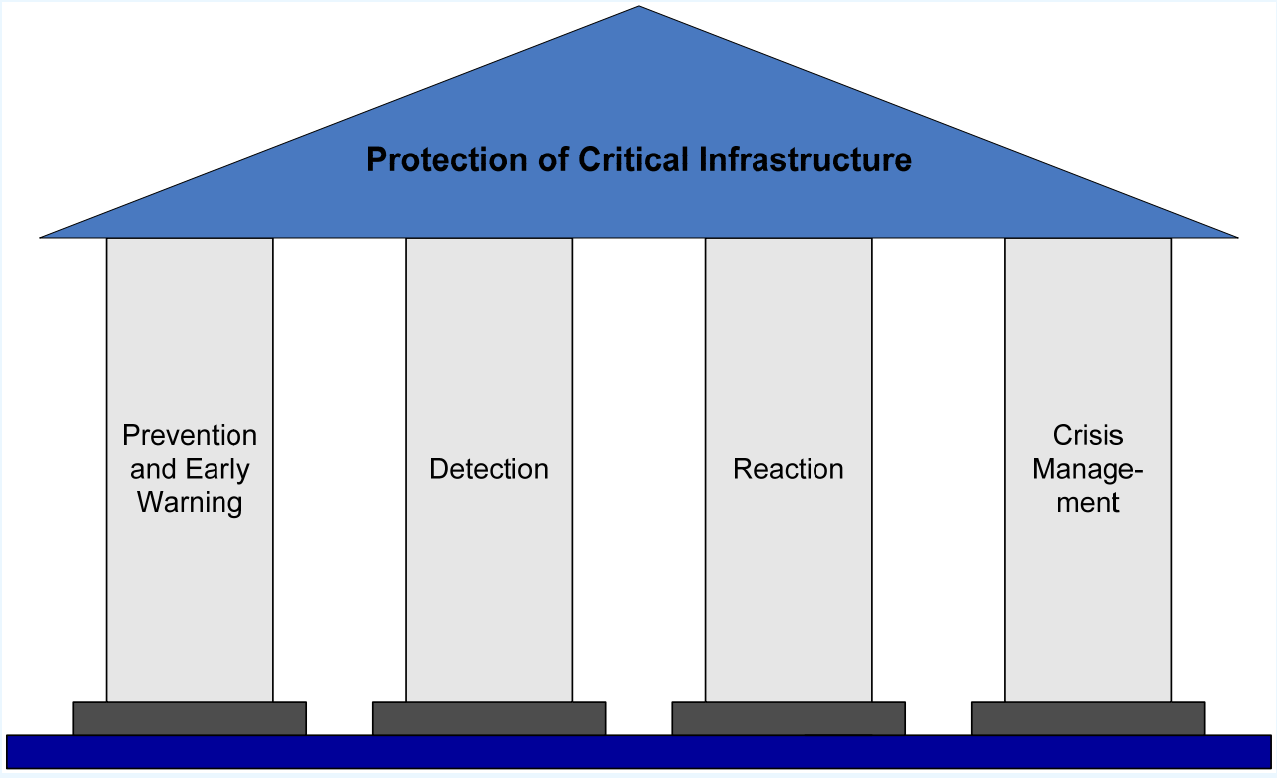
Within the administration, the CIIP unit should act as the center of competence for all questions related to information security. Since information security concerns many different agencies, the CIIP unit should cooperate with various partners within the government. Hence, crisis management needs to be rehearsed regularly. A well-designed crisis management plan is of no use, if it does not work in emergencies. The CIIP unit should conduct exercises with other governmental crisis organizations and CI operators repeatedly. All crucial actors must be familiar with their responsibilities, duties, and risks in times of crisis.

In particular, the CIIP unit should raise awareness of the various existing interdependencies. Operators of CI are dependent on each other in many respects. For instance, energy supply is crucial for the communication sector and vice versa. Since companies may tend to focus on their own business, they may often lack awareness of these interdependencies. The government in turn may also neglect the fact that it is dependent on the functioning of these critical infrastructures. A key task for the CIIP unit is to reinforce understanding of these dependencies among different actors: for example, through workshops and exercises. CIIP can only succeed if all stakeholders work together, with the same goals.

2.5 Illustration of the Four-Pillar Model

Figure 1 summarizes illustrates the four pillars of CIIP:

Figure 1: The Four Pillars of CIIP



3 Essential Partners: The Cooperation Model

Given its involvement across the four pillars, and the challenges they pose, the CIIP unit has to have different specialized competencies, implying a large and complex organization. However, the CIIP unit can be streamlined without loss of capacity by establishing cooperation among different partners who are best qualified to cope each with one of the tasks. If each partner concentrates on their competency, existing know-how can be applied most efficiently, saving costs, as well as manpower. According to the tasks of each of the four pillars, CIIP requires different organizational, technical, and analytical competencies. The CIIP unit should ideally include three partners:

- A governmental agency, providing strategic leadership and supervision (the Head of the CIIP unit),
- An analysis center with strong linkages to the intelligence community (the Situation Center),
- A technical center of expertise, usually consisting of staff members of a national CERT (the CERT Team).

This section describes these partners and examines which partner should provide which services to form an effective CIIP unit.

3.1 Strategic Leadership and Supervision

The CIIP unit needs a responsible authority to provide strategic leadership and supervision, the "head of the CIIP unit" which should be part of the state administration. However, since CIIP concerns most sectors of government, the CIIP unit could be positioned within several different governmental agencies. As Myriam Dunn writes: "The establishment and location of these key organizations within the government structures are influenced by various factors such as civil defense tradition, the allocation of resources, historical experience, and the threat perception of key actors in the policy domain."[10] Nevertheless, there are some requirements for the head of the CIIP unit, and some agencies are better adapted to the tasks of CIIP than others.

First, the designated head of the CIIP unit should have a background and strong qualifications in ICT (particularly, information assurance) or in critical infrastructure protection. These issues involve various different organizations and agencies, ranging from emergency planning and disaster response organizations to data security and high-tech crime units.[11]

Due to the different options for the location of the CIIP unit within the government structure, there is a danger of inter-bureaucratic conflicts among different stakeholders. To avoid obstruction, the CIIP unit should be located in a well-established agency to ensure that the importance of CIIP is acknowledged by policy-makers.

Finally, it is essential that the head of the CIIP unit enjoys the confidence of the private sector. The need for Public-Private Partnerships (PPP) was recognized by the report of the President's Commission on Critical Infrastructure Protection (PCCIP) in 1997.[12] Nevertheless, implementation of PPP is not always easy. Malm and Anderson write: "It is relatively easy for a government and private actors in a PPP to agree that there is a problem and that something must be done to resolve it. It is much harder, however, to agree on what should be done, who should be responsible for doing it, and who should assume legal responsibility, as well as the financial cost involved in implementing new measures."[13] Since cooperation between public and private stakeholders is often difficult, experienced negotiators are required. The agency where the CIIP unit will be located should be accustomed to interacting with the private sector. Furthermore, since private firms will only share sensitive commercial and security information when they trust their partners,[14] the location of the CIIP unit is often constrained by the need to assure private companies that their sensitive information will be adequately safeguarded.[15]

---

[10] Dunn, Myriam (2005): A Comparative Analysis of Cybersecurity Initiatives Worldwide, paper presented at the ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 2005), p. 15.
[11] Abele-Wigert, Isabelle and Myriam Dunn (2006): International CIIP Handbook 2006, Vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies (Zurich: Center for Security Studies), pp. 394–8.
[12] President's Commission on Critical Infrastructure Protection (PCCIP) (1997): Critical Foundations: Protecting Americas Infrastructures (Washington, DC: White House), pp. 27ff.
[13] Andersson , Jan J. and Andreas Malm (2006): Public-Private Partnerships and the Challenge of Critical Infrastructure Protection , in: Dunn, Myriam and Victor Mauer (eds.): International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects (Zurich: Center for Security Studies), pp. 166f.
[14] Branscomb, Lewis M. and Erwann O. Michel-Kerjan (2006): Public-Private Collaboration on a National and International Scale, in: Philip E. Auerswald et al. (eds.): Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability (Cambridge: Cambridge University Press), pp. 396ff.
[15] Dunn, 2005: p. 17.

3.2 Analytical Capacity

The gathering and analysis of threat information are demanding tasks, requiring a broad network of national and international contacts. It could prove inefficient if the CIIP unit established its own intelligence unit. Instead, the task of analyzing threat information could be allocated to specific units of the intelligence services. Their international networks and experience in international investigation are invaluable in the fight against cyber-crime. In order to cooperate in the most efficient way, specific units of the intelligence services should cooperate with the CIIP unit as partners. In an ideal scenario, the leader of the analysis sub-unit could be a staff member of the intelligence service, acting as an interface between the CIIP unit and the intelligence service

In the following, this sub-unit will be labeled the "Situation Center", in order to highlight its functions of gathering and analyzing threat information.

3.3 Technical Competencies

In many countries, CERTs[16] are responsible for the technical questions of information security.[17] The role of CERTs can be compared to that of a fire department. They are ready to help in case of incidents, but also engage actively in prevention by providing information, warnings, and advice to their constituencies.[18] The size of CERTs and of their constituencies varies widely, but despite their differences, all CERTs are designed as centers of expertise run by information specialists.

Following the example of the first CERT at Carnegie Mellon University, many CERTs tend to be located outside the government. Often, they are run by agencies that are completely independent from the government. CERTs operated by universities are particularly interesting, as they have two major advantages: First, the scientific staff of universities are more likely to cope with the complex research in the fields of information technology and network environments. Second, the universities' academic networks are very useful for research and cooperation with the CIIP unit. Regardless of who runs the CERTs, the CIIP unit should closely cooperate with the CERTs. Moreover, the CIIP unit should try to integrate an established national CERT as a partner. In this way, the CIIP unit can gain technical competence, without having to build up its own body of technical staff. The integrated CERT will subsequently be referred to as "CERT Team" of the CIIP unit.

3.4 Conclusion: the Tripartite Composition of the CIIP Unit

In summary, the CIIP unit would include the three partners of the head of the CIIP unit for leadership, the Situation Center for analysis and information and the CERT team providing technical expertise. Figure 2 summarizes the tripartite relationship involved in an integral CIIP approach.

[16] Another often-used name is Computer Security Incident Response Team (CSIRT), but there are other terms and acronyms. For further information, see Killcrece, Georgia et al. (2003): State of the Practice of Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Pittsburgh University Press).
[17] For a list of existing CERTs all over the world, see www.first.org/members/teams/.
[18] West Brown, Moira J. et al. (2003): Handbook for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Pittsburgh University Press), p. 2.

Figure 2: The Tripartite Composition of the CIIP Unit

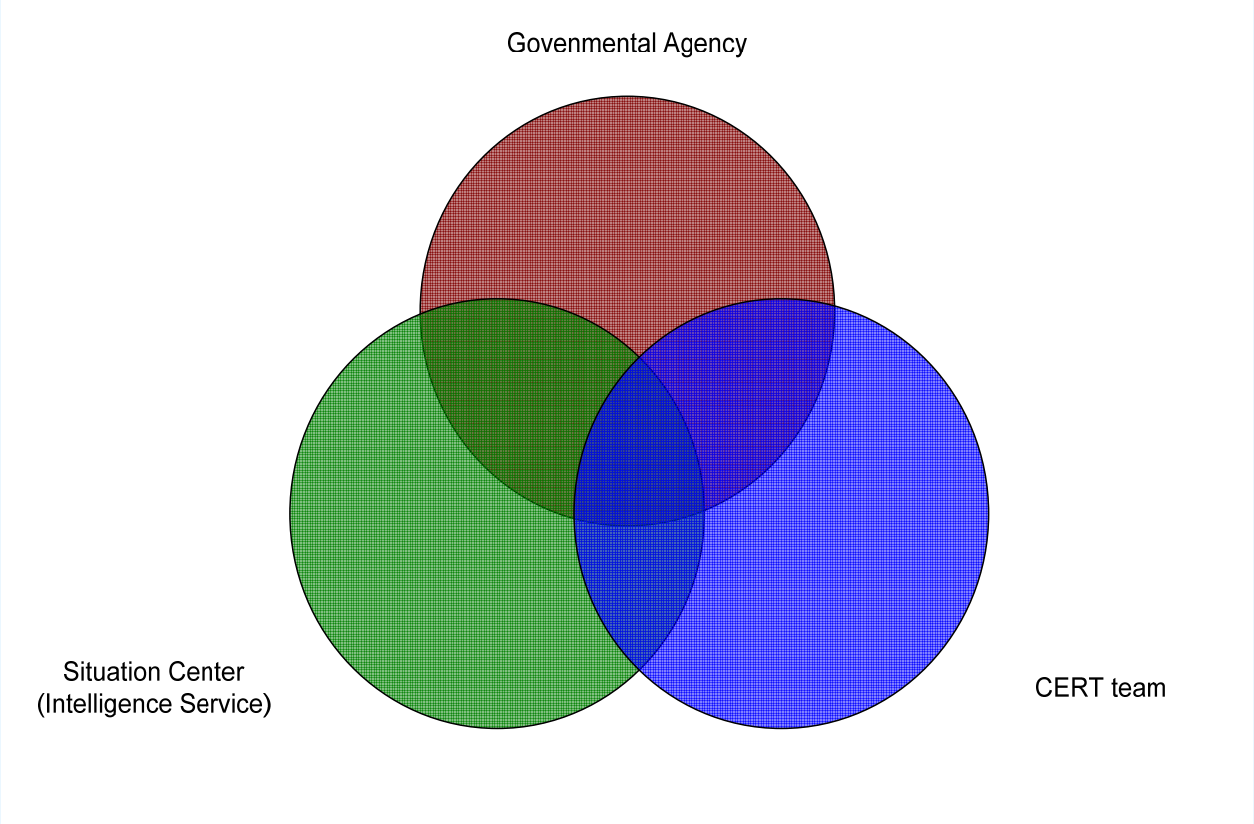


Figure based on Henauer 2004, p. 130.

4 ORGANIZATION OF THE CIIP UNIT

The tripartite composition of the CIIP unit has many advantages; however, these advantages can only be exploited to best effect when the CIIP unit is well-organized. It is therefore worth examining the internal structure of an optimally functional CIIP unit. The organizational chart presented in Figure 3 highlights the structure of the CIIP unit. The absence of many levels of hierarchy allows direct communication and effective cooperation. It is also crucial to establish clear responsibilities and duties for involved partners.

Figure 3: The Organizational Chart of the CIIP Unit

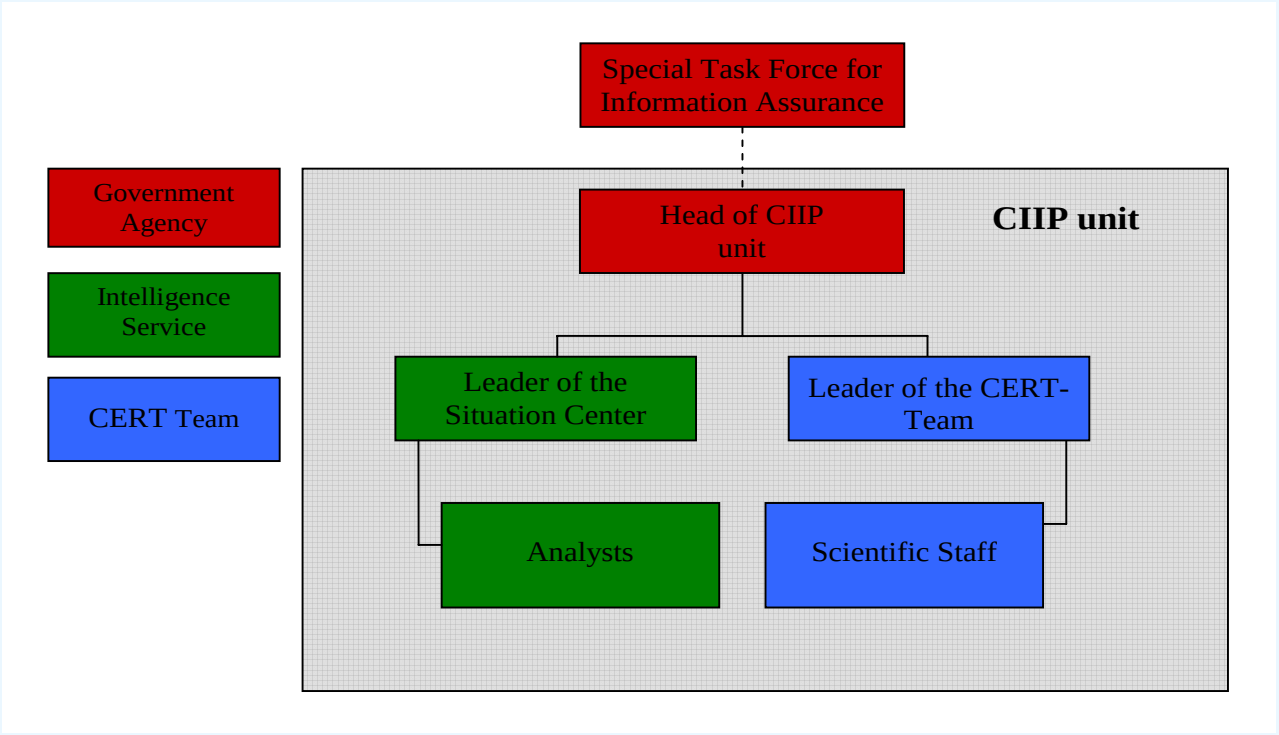


Figure based on Rytz 2007, p. 9.

As mentioned previously, the CIIP unit should be located within a well-established government agency. In practice, this agency provides the head of the CIIP unit, a person who represents the unit in public, as well within the administration. In order to understand the complex problems of companies, the person in question should be experienced in the area of information security regarding critical infrastructures. On the other hand, the person should be competent in dealing with the administration and in communicating with the public. The leader of the CIIP unit may have one ore two deputies; nevertheless, the task of strategic leadership can basically achieved by one person.

In crisis situations, the CIIP unit leader's responsibilities will change. In emergency scenarios, a Special Task Force for Information Assurance should be established, comprising relevant decision-makers from the public and private sectors. The leader of the unit must then remain in contact with this task force and ensure that the CIIP unit works directly for the task force.

In close cooperation with the head of the CIIP unit, the Situation Center assumes the non-technical tasks. The leader of the Situation Center serves as the interface with the intelligence community. The leader and his or her team evaluate new threats, refer targets to the prosecution authorities, and supply the public with relevant information. The leader of the Situation Center does not have to be an expert in information security, but should have considerable legal and political knowledge. The Situation Center performs the major tasks of the CIIP unit: it is responsible for mentoring the operators of CII, and should help to raise public awareness.

Finally, the leader of the CERT team must have a thorough knowledge of information assurance, as the CERT team is responsible for technical questions. Since prevention and early warning are essential tasks of the CIIP unit, the head of CERT should have scientific qualifications, but also be skilled in communicating. As mentioned above, the CIIP unit does not need to form its own CERT, but should try to integrate an established national CERT (e.g., a CERT run by a university). In this way, the CIIP unit can rely on existing knowledge within the CERT and minimize manpower requirements.

Table 1 summarizes the required skills of the leaders of the CIIP partners, according to their positions:

Table 1: Required Skills of the CIIP partners

Position	Required Skills
Leader of the CIIP unit	Experienced in the area of information security With good contacts with policy- and decision-makers Communication and representation skills
Leader of the Situation Center	Profound legal and political knowledge Linked to intelligence services Experienced in the work of prosecution
Leader of the CERT team	Extensive technical skills Teaching and communication skills Member of an established national CERT

5 THE NETWORK OF THE CIIP UNIT

In order to accomplish the demanding tasks described in Section 3, each sub-unit of the CIIP unit needs to be embedded in a broad network of national and international partners. Each sub-unit has different contacts according to its respective tasks. This section clarifies which sub-unit is responsible for building up contacts with different partners.

Obviously, the most important partners of the CIIP unit are the owners and operators of critical information infrastructures. The design of these public-private partnerships will be described in Section 6. This section describes partners who do not directly operate CII, but whose contributions to CIIP are essential.

5.1 Partners of the Head of the CIIP Unit

First, the head of the CIIP unit should have well-established contacts to all other governmental agencies engaged in CIIP. Since CIIP concerns diverse divisions of the administration (e.g., divisions of economic supply, civil protection, military defense, communication, etc.), there are many different administrative activities that relate to CIIP. The head of the CIIP unit should be familiar with the activities of other administrative units and strive to pool existing resources. This task is difficult, because different agencies have different or even contradictory viewpoints. In addition, civil service bureaucracies do not like sharing responsibilities with other administrative units – there is, as mentioned above, a danger of inter-bureaucratic conflicts. Thus, the partnership among all agencies involved with CIIP has to be constantly renewed and reaffirmed under the lead of the CIIP unit.

Apart from pooling the existing administrative resources, the head of the CIIP unit also has to cooperate with partners outside the administration. Over recent years, many initiatives have emerged from the private sector. It is in the interest of many companies (e.g., IT manufacturers, software producers, banks, insurances, business associations, media, etc.) to raise the awareness of private users and to enhance user confidence in new technologies.[19] The head of the CIIP unit should actively promote cooperation with these actors. In their own interests, these companies undertake the tasks of spreading information. The CIIP unit should support and complement those initiatives by providing expert information.

Of course, the head of the CIIP unit should cooperate not only with national partners, but also with the CIIP units of other countries. Since threats to information security surpass geographical borders, international cooperation is essential for a successful protection of CII. The CIIP units of different countries can exchange experiences and learn from each other.

[19] Some examples of private associations dedicated to information security and awareness-raising are given at: http://www.enisa.europa.eu/pages/09_03.htm.

5.2 Partners of the Situation Center

In order to achieve the tasks of gathering and analysis of information, and connecting targets with law enforcement, the Situation Center needs to establish close contacts with other units of the intelligence service, the police (in particular the high-tech crime units), and with foreign intelligence services. In this context, offices for cyber-crime (usually operated by police) are of particular importance.[20] Such offices are an appropriate venue for the public to report suspect activities concerning the Internet. For the analysts of the CIIP unit, these reports are valuable sources that may reveal new vulnerabilities or provide evidence for attacks. Hence, a close partnership between the Situation Center of the CIIP unit and these offices for cyber-crime is vital.

With regard to prosecution after an incident, contacts with foreign intelligence services and police units are very important. While the head of the CIIP unit should cooperate with CIIP units of other countries on a strategic level, the team of the Situation Center works alongside them (for example, there are several working groups of Interpol that are charged with combating information technology crime,[21] but there are many more platforms of cooperation among the intelligence services and police units). In practice, such networks are very useful, particularly in supporting prosecution authorities, which may lack experience in investigating Internet fraud.

5.3 Partners of the CERT Team

Since new vulnerabilities and new forms of attacks evolve almost daily, incident response and the technical protection of large networks are highly demanding. The CERT team needs to be constantly updated on new developments and needs a broad network of contacts with cyber-security experts. In order to learn about potential vulnerabilities, it should establish contacts with IT manufacturers and software producers.

International exchange of information about incidents is also crucial for the CERT team. If every CERT tried to elaborate its own response to a particular incident, they would always be too slow. Global security incidents can be handled most successfully, if the CERT teams of different countries work together. The Forum for Incident Response and Security Teams (FIRST)[22] is an important platform for exchange. FIRST defines its aims as follows: “Resolution of any computer security incident generally involves many sites, which may be located in various places around the world. Each incident response and security team can assist their local constituency and coordinate the appropriate response with other teams to provide a global solution to the problem. […] Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.”[23]

Since national and international cooperation is pivotal for technical protection, it is vital that the CERT team of the CIIP unit should be a member of FIRST and strive for close partnership with other national and international technical experts.

5.4 The Network of the CIIP Unit

National and international contacts of the CIIP unit are key elements of effective CIIP. Each sub-unit brings its own partners into the CIIP unit and maintains these contacts in coordination with the CIIP unit. In this way, the unit becomes embedded within the national network and can rely on support from other agencies different actors. Figure 4 illustrates the network of the unit:

[20] See, for example, the Cybercrime Coordination Unit Switzerland: http://www.kobik.ch/index.php?language=en.
[21] See: http://www.interpol.int/Public/TechnologyCrime/default.asp.
[22] See: http://www.first.org.
[23] See: http://www.first.org/about/mission/mission.html.

Figure 4: The Network of the CIIP Unit

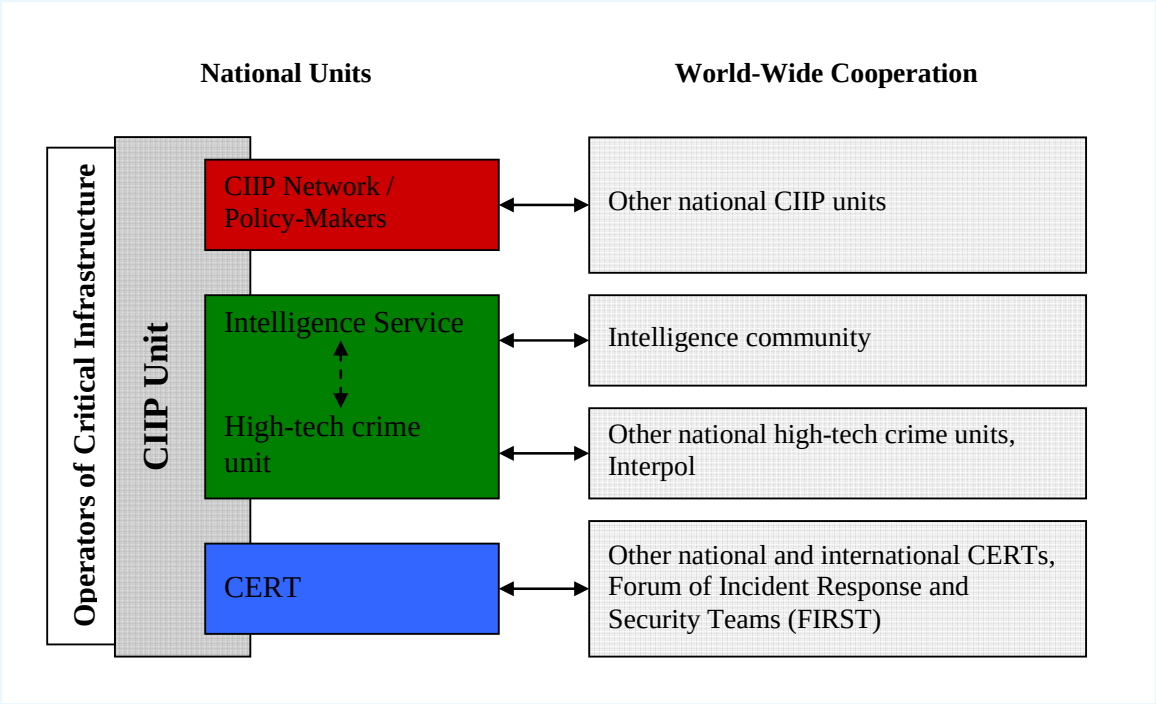


Figure based on Rytz 2007, p. 15.

6 CUSTOMERS AND PRODUCTS

In addition to the structure of the CIIP unit, it is equally important to define the CIIP unit's audience. Most importantly, the CIIP unit must serve the owners and operators of CII. However, in the fight against cyber-crime, it is also vital not to neglect private users, SMEs, and other businesses. As mentioned, ICT by its very nature is a highly networked arrangement. Overall security can only be promoted if awareness of this problem is raised among all ICT users. In consequence, the CIIP unit serves two broad customer groups:

- the Closed Customer Base (CCB), including operators of nationally critical infrastructures; and
- the Open Customer Base (OCB), including all other companies (in particular SMEs), as well as home computer users.

These two customer bases have very different needs. Accordingly, the CIIP unit must provide different products and services tailored to each group. This section discusses the different products and services tailored to the Closed Customer Base, and secondly, to the Open Customer Base.

6.1 The Closed Customer Base (CCB)

The Closed Customer Base consists of operators of critical infrastructure. Since these companies usually have strong competencies in ICT security, employ their own specialists, and are able to mobilize know-how and financial resources to protect their systems, they are only mildly interested in general advice about information security. Instead, these operators are looking for specific, specialized information on emerging threats and new risks. For CI operators, cooperation with the CIIP unit is only attractive if the CIIP unit is able to provide exclusive information and services.

The CIIP unit itself, in turn, depends on receiving information from these companies. In order to maintain the services of critical infrastructures without interruption and to be informed as soon as possible of major incidents, the CIIP unit needs to receive information from the operators of critical infrastructure continuously. Close, equitable cooperation between the operators of CI and the CIIP unit is thus essential.

This Section discusses which services and products the CIIP unit should provide in order to foster Public-Private Partnerships, how information-sharing with and within the CCB may be established, and the chances and challenges of such cooperation. But first, the design of the closed customer base is discussed.

6.1.1 The Design of the Closed Customer Base

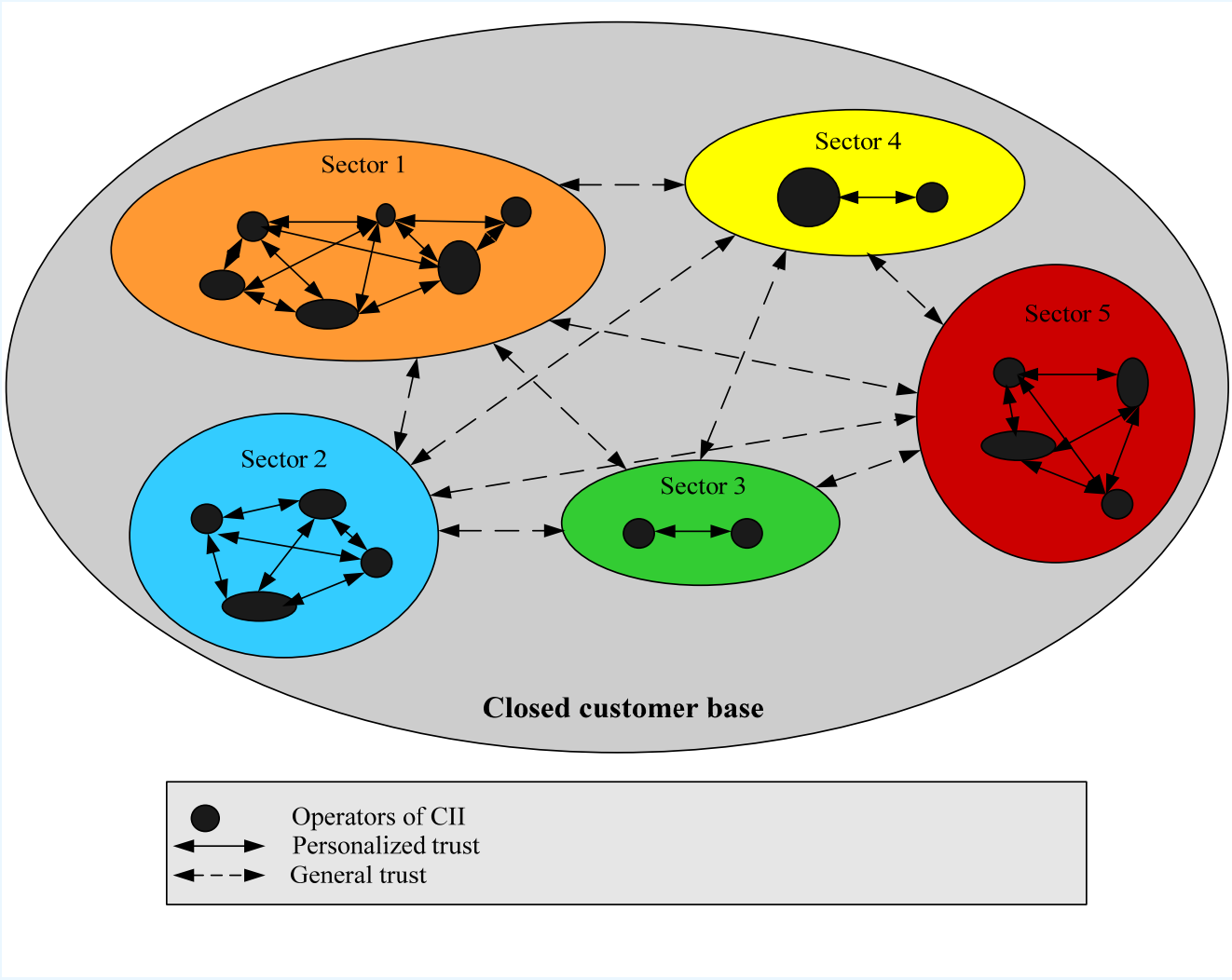
Membership of the CCB is restricted to operators of CI. However, definitions of critical infrastructures vary across countries. Some countries have followed the example of the US Presidential Commission on Critical Infrastructure Protection (PCCIP), which was the first governmental agency to define critical sectors,[24] while others have developed methods and criteria to identify critical sectors.[25] Nevertheless, some key infrastructures (e.g., Energy/Electricity, Health Services, Communication, Government Services, Banking and Finance, Emergency/Rescue Services, Transportation, Water Supply) have generally emerged as critical elements in almost all countries.[26] Further, since criticality is an evolving concept, the CIIP unit should focus on integrating into the CCB companies belonging to critical sectors, and remain open to integrating other sectors later.

Apart from the question of the critical status of various sectors, the size of the closed customer base has to be considered carefully. As discussed below, the exchange of exclusive information – the key element of the closed customer base – presupposes mutual trust. Building up that trust is very difficult, and once established, it remains fragile.[27] Trust needs to be cultivated constantly. In one of the first evaluations of the success of the Information Sharing and Analysis Centers (ISACs)[28] in the US, the General Accounting Office wrote: "All of the organizations agreed that trust had to be built over time and through personal relationships…"[29] This implies that the number of members of the CCB should be kept to a manageable size (in order to enable personal relationships) and that membership should be as constant as possible. It is therefore advisable for the CIIP unit to limit the numbers of representatives per company.

In addition, the CCB should be separated into different sectors, according to the different types of infrastructures (e.g., financial sector, sector of energy supply, telecommunication sector, etc.). Not all information has to be shared with all members (options for keeping information classified within the closed customer base are discussed below), and it is often beneficial to restrict some meetings, workshops and/or exchanges of information. Figure 5 outlines the design of the closed customer base, including miscellaneous relationships among particular companies.

[24] President's Commission on Critical Infrastructure Protection (PCCIP), 1997.
[25] For examples of how to determine which sectors are critical, see: Dunn, Myriam, and Isabelle Wigert (eds.): CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries (Zurich: Center for Security Studies, 2004), pp. 229–32.
[26] Abele-Wigert and Dunn (2006): 385–94.
[27] Prieto, Daniel B. (2006): Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects, in: Philip E. Auerswald et al. (eds.): Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability (Cambridge: Cambridge University Press), pp. 404–28.
[28] For further information about ISACs, see for example: Dacy, Robert F. (2004): Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors (Washington, DC: United States General Accounting Office).
[29] United States Government Accountability Office (GAO) (2001): Information Sharing: Practices That Can Benefit Critical Infrastructure Protection (Washington DC, United States General Accounting Office), p. 7.

Figure 5: The Design of the Closed Customer Base



6.1.2 Products and Services for the Closed Customer Base

In order to support operators of CI, the CIIP unit should provide the following services to the members of the closed customer base:

- *Assistance in case of incident:* This is the most important task of the CIIP unit. The key element is a 24/7 on-call service. Since time is a vital factor in countering attacks, and given that many attacks are carried out at the week-ends or at night, the CIIP unit must be able to support the operators of CI at any time of the day or night. Since the CIIP unit involves three different partners, it can act as a *one-stop shop* for members of the closed customer base that are affected by an incident. It can provide technical advice and support, put the targets of an attack in touch with the appropriate law enforcement authorities, and make its broad national and international network available to the members of the CCB.
- *Distribution of exclusive information:* Thanks to its intelligence-analysis capabilities and its CERT team, the CIIP unit can compile threat analyses, situation reports, statistics, background information, and perpetrator profiles, and make them available to the operators of CI. In this way, for example, a threat of economic espionage can be communicated directly to key representatives of the private sector. For disseminating warnings, advice and information, it may be useful to operate an online platform (of course, this platform should be both secure and reliable).
- *Workshops, meeting, exercises:* In order to foster trust and reinforce knowledge of specific issues, the CIIP unit should organize workshops, meetings, and exercises on relevant issues with added

value for the CCB a regular basis. Depending on the issue, these workshops may be conducted solely for members of one sector, or may be open to the entire membership of the CCB.

6.1.3 Information-Sharing among Members of the Closed Customer Base

Apart from the services of the CIIP unit, members of the Closed Customer Base can also profit from each others' knowledge and experiences. The idea of information-sharing among operators of critical infrastructures was included in the 1997 report of the President's Commission on Critical Infrastructure Protection (PCCIP). It was suggested to "provide an information-sharing and analysis capacity to support [corporate] efforts to mitigate risk and effectively respond to adverse events, including cyber, physical and natural events."[30] The need for information-sharing became all the more obvious when it became clear that attackers exchange information and experiences almost constantly over online platforms.

Since the operators of CII are experienced professional providers of ICT infrastructures, considerable know-how can be gained through exchanges of experiences, recommendations, standards and best practices among ICT experts, enabling them to react rapidly and adequately to evolving threats to information security.[31] In addition to the advantages of information-sharing, there are however formidable obstacles. First, CI is often operated by companies competing with each other. They may fear the misuse of shared information by their competitors, or they may not be willing to share information due to rivalry. Aviram and Tor point the negative consequences of the rivalrous nature of information for the likelihood of information-sharing: "The axiom that sharing information among competitors […] is non-rivalrous is a gross oversimplification. An analytical framework that fails to take into account the private cost to a firm of allowing its competitor to benefit from an information exchange […] will overestimate the likelihood of information sharing."[32] Companies may be very reluctant to share any information with their competitors.

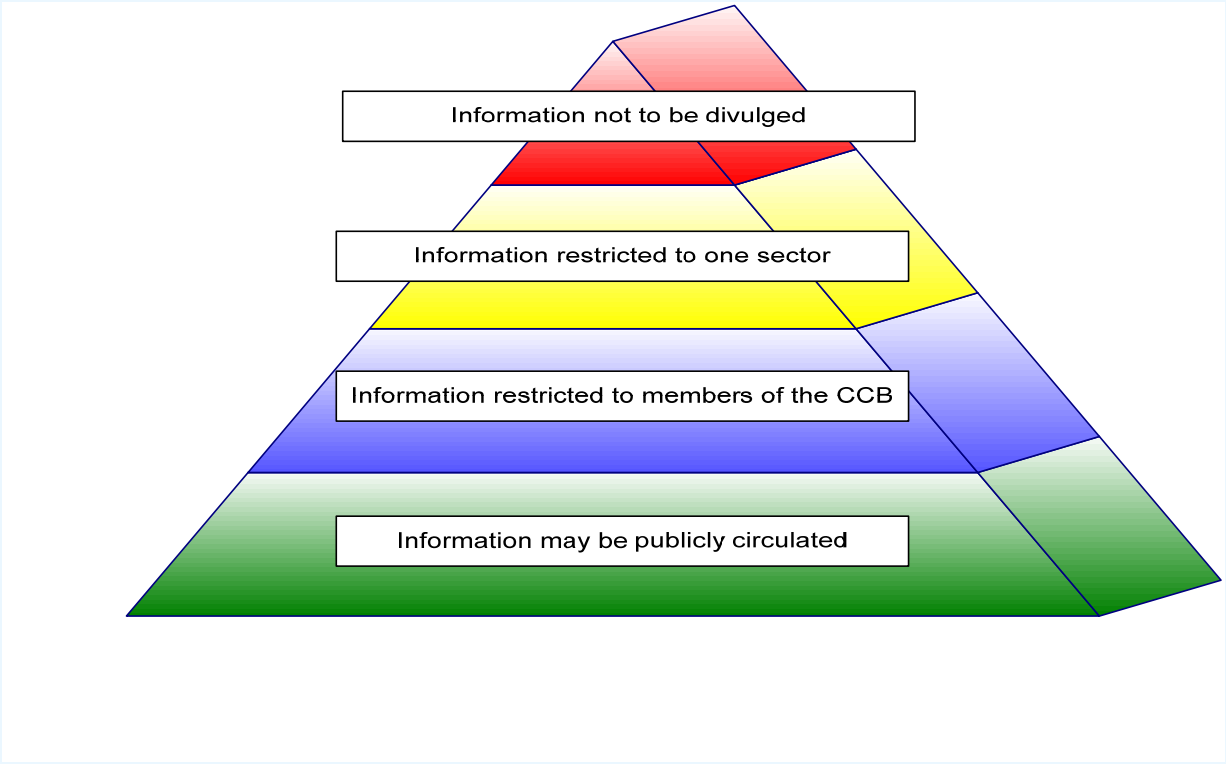
Second, information-sharing in information security is especially sensitive for companies. Usually, information about their IT systems are among their best-guarded secrets. As Harris Miller of the Information Technology Industry Association of America (ITAA) points out, "You're not talking about companies sharing their advertising and marketing material, you're taking about sharing their deepest, darkest secrets."[33]

Strong mutual trust is an absolute condition for any information-sharing efforts. It is one of the key tasks of the CIIP unit to foster trust among operators of CI. Trust may be formed on a personal basis by meetings and workshops, particularly by smaller meetings among companies of the same sector. Nevertheless, in order to guarantee the integrity of shared information, formal agreements are needed. All members of the CCB, as well as all partners of the CIIP unit, should sign a non-disclosure agreement to guarantee that information is subject to the control of the source company divulging it to the other members. Without the explicit permission of the source company, neither the CIIP unit nor other members of the CCB are allowed to forward information to state authorities, other companies or the public.

In order to be an efficient and trustworthy platform for information-sharing, the CIIP unit should offer a variety of classification levels for information. Each company should be able to decide with whom it wishes to share information. Figure 6 shows the different potential classification levels for information.

[30] United States Government Accountability Office (GAO) (2004): Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors (Washington DC, General Accountability Office), p.8.
[31] Holderegger (2006): p. 125.
[32] Amitai, Aviram and Avishalom Tor (2003): Overcoming Impediments to Information Sharing, in: Alabama Law Review, no. 55, p. 243.
[33] Poulsen (2005).

Figure 6: Classification levels



These classification levels enable companies to limit the spread of information. Of course, it should always be the information source who decides on the classification, and the information may only be re-classified with their agreement. This rule is fundamental and should be observed at all times. The CIIP unit has to be aware of the fact that it takes a long time to build up trust; however, this trust may be destroyed very easily: "when trust built over long-term relationships is lost, it is extremely difficult to restore."[34]

In order to enable information-sharing, legislative measures may be necessary. States have enacted laws to prevent the building of trusts in favor of free competition. Such legislation may now hamper information-sharing and may have to be reviewed. For instance, US antitrust agencies have facilitated the compliance of Information Sharing and Analysis Centers (ISACs) with anti-trust laws by issuing "business review letters" in which they state that they have no intention of challenging the ISAC.[35] In the same way, legislation on the disclosure of information is also important. Information-sharing is more likely where the information-sharing association is exempt from disclosure under state and local laws.[36] Therefore, the CIIP unit should strive to promote legislation to create "safe harbors" of information-sharing.[37]

6.1.4 The Closed Customer Base as Public-Private Partnership: Chances and Challenges

Information-sharing and mutual support between government and private companies is seen as the best and most sustainable way of protecting CI. Consequently, close collaborations – usually referred to as a Public-

[34] Branscomb and Michel-Kerjan (2006): p. 397.
[35] Personick, Stuart D. and Cynthia A. Patterson (eds.) (2003): Critical Information Infrastructure Protection and the Law: An Overview of Key Issues (Washington, DC: National Academic Press), pp. 17–34. For a list of business review letters, see: http://www.usdoj.gov/atr/public/busreview/letters.htm.
[36] Amitai, Aviram (2005): Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations, in: Grady, Mark and Francesco Parisi (eds.): The Law and Economics of Cyber-Security (Cambridge: Cambridge University Press), p. 149.
[37] Cukier, Kenneth N., Viktor Mayer-Schoenberger, and Lewis M. Branscomb (2005): Ensuring, (and Insuring?) Critical Information Infrastructure Protection (KSG Working Paper), p. 17.

Private Partnerships (PPP) – have been established in many countries.[38] However, as mentioned previously, PPPs are not always easy to establish, as they are time-consuming, cost money, and require consensus among actors.[39] Private companies may be reluctant to join the PPPs, or even worse, they "simply participate in PPP as a means to deflect attention from insufficient emergency-preparedness measures and to avert outright regulation."[40]

The CIIP unit therefore has to provide incentives to make collaboration attractive to CII operators, by providing efficient and effective support, offering exclusive information and connecting companies with each other. In order to be successful, the CIIP unit must handle all incidents in a discreet and trustworthy manner. Nevertheless, the CIIP unit cannot prove its value until some companies have entered into partnership. Initially, building up the CCB is a major challenge. The CIIP unit should first identify a champion inside each sector, and persuade this champion to join the CCB. Later, these champions can advise the CIIP unit on how to contact other companies and can help to persuade them to join the CCB. In this way, the CCB grows successively – provided that partnerships are not misused.

If the CIIP unit successfully establishes a CCB, the next challenge is to limit membership in the CCB. As mentioned above, the CCB should not involve too many companies, because trust is often based on personal relationships. The CIIP unit has to define the limits of the growth of the CCB. This means that it should focus on companies operating the most important infrastructures. It may be necessary to refuse membership to other companies – an awkward step for any governmental unit. Therefore, plans should be developed for other forms of cooperation with these companies.[41] In addition, if the CIIP unit proves successful, the CCB may expect too much from it. Once the operators of CII have noticed that the CIIP unit is able to provide effective and efficient support, they may tend to rely on that support and reduce their own efforts. Therefore, the CIIP unit has to define its responsibilities clearly and explain what activities it can undertake (and why) and what activities it cannot.

6.2 The Open Customer Base (OCB)

Since every insecure computer connected to the Internet threatens the security of all other connected computers, the activities of the CIIP unit must also address the broader public. Of course, the CIIP unit cannot provide the same services to the Open Customer Base (OCB) as it provides to the Closed Customer Base. In particular, the CIIP unit cannot assume all necessary prevention tasks, since this would stretch the unit far beyond its resources. This section discusses which of the potential services for the broad public may be achieved by the CIIP unit. However, providing these services and products is not straightforward, because for governmental agencies, public activity involves always public responsibility. If the CIIP unit undertakes efforts to raise public awareness, it risks being expected to deal with a wider range of tasks related to information security and cyber-crime. This problem is discussed in the second part of this section.

6.2.1 Services and Products for the Open Customer Base

Possible tasks of the CIIP unit in serving the OCB include awareness-raising, warning and assistance in case of incidents.

- *Awareness-raising:* The European Network and Information Security Agency writes: "As it is […] the human component that is critical in any effective and robust security framework, any initiative to increase the awareness of ICT users so as to positively influence their secure behaviour, should have

[38] Abele-Wigert and Dunn, (2006): p. 393.
[39] Andersson and Malm (2006): p. 151.
[40] Dunn, Myriam and Victor Mauer (2006): Introduction, in Dunn, Myriam and Victor Mauer (eds.): International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects (Zurich: Center for Security Studies), p. 20.
[41] For example, the CIIP unit can support and promote the establishment of privately-managed communities where members can receive and share up-to-date advice, information and experiences. In the UK, the Centre for the Protection of the National Infrastructure (CPNI) has developed such a model. The CPNI provides comprehensive support for the formation and operation of so-called Warning Advice and Reporting Points (WARPs), without entering into direct partnerships with the members of these WARPs. For more information on information-sharing with SMEs, see Suter, Manuel (forthcoming): Improving Information Security in Companies: How to Meet the Need for Threat Information, in Myriam Dunn, Victor Mauer, and Felicia S. Krishna-Hensel (eds.): Power and Security in the Information Age: Investigating the Role of the State in Cyberspace (forthcoming 2007, Ashgate).

a significant effect on mitigating information security-related incidents."[42] As a center of expertise, the CIIP unit can create greater awareness about information security. The CIIP unit can disseminate basic knowledge on information security. Many users feel overwhelmed by the complexity of information security. The CIIP unit can provide simple and reliable information, for example, through its website. It should compile a glossary of the most important terms and definitions, provide information about the most frequent types of attacks and present checklists, configuration instructions, and recommendations for the safe use of different ICTs. In addition, the CIIP unit can conduct and present studies and situation reports for the broader public.

- *Warnings and guidance:* Over the recent years, IT security has evolved into a business area in its own right. Many security consultants and computer periodicals issue regular warnings and publish information on new security gaps. While such warnings and advice may be relevant for IT professionals, they usually overwhelm the average IT user.[43] To support these users, the CIIP unit could filter the bulk of warnings and convey selective warnings and guidance, tailored to the needs of amateurs. For instance, warnings may be conveyed "when measures become necessary that go beyond the basic protection recommended in the configuration instructions, which would massively reduce the frequency of warnings."[44] These warnings may be published on the website of the CIIP unit and disseminated through a freely available newsletter or through the media.
- *Assistance in case of incidents:* It is not easy for the CIIP unit to define the form and scope of assistance for SMEs and citizens. On the one hand, the security of the general public is in the interest of the CIIP unit. Every reported incident increases the flow of information and enhances the early-warning capability of the CIIP unit (for instance, users of e-banking services who discover suspect withdrawals from their account may report attempts of phishing attacks[45], before they are detected by the bank). On the other hand, it is clear that the CIIP unit cannot attend to all potential incidents or handle the viruses and spam mail problems of private users. However, due to the importance of monitoring attacks, the CIIP unit should host an option to report incidents (for example, over an online reporting form) or, as mentioned in Section 5, work together with the cyber-crime units of the police that provide such reporting services for the public. Of course, comprehensive assistance would not be possible, but the CIIP unit can support targets of attacks by answering technical questions and/or giving legal advice.

6.2.2 Opportunities and Challenges of the Open Customer Base

With regards to the OCB, the CIIP unit faces two major challenges: first, it has to deal with the highly heterogeneous nature of the potential customer base, and secondly, it may be confronted with exaggerated expectations on the part of the public. Neither of these problems has a direct impact on the daily work of the CIIP unit (the protection of the critical infrastructures); however, with regard to the unit's public relations and reputation, they have to be taken seriously.

Threats to information security affect different users to very different extents. Whereas private users are mainly affected by viruses, worms, Trojan horses, spyware or spam mails, firms (in particular large businesses) often suffer targeted attacks on their IT infrastructure.[46] Hence, the requirements of the users

[42] European Network and Information Security Agency (ENISA) (2005): Raising Awareness in Information Security: Insight and Guidance for Member States, p. 4. URL: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf

[43] Holderegger (2006): 123.

[44] Ibid.

[45] The word "phishing" is a contraction of the words "Password", "Harvesting", and "Fishing". Fraudsters phish in order to gain confidential data from unsuspecting internet users. This may, for example, be account information from online auctioneers (e.g., eBay) or access data for internet banking. The fraudsters take advantage of their target's good faith and helpfulness by sending them e-mails with false sender addresses. The e-mails tell the targets, for example, that their account details and access data (e.g., user name and password) are no longer secure or up-to-date and need to be changed at the link provided in the e-mail. The link, however, does not lead to a genuine page provided by the apparent service provider (e.g. the bank), but the fraudster's apparently identical web page. (Definition from: http://www.melani.admin.ch/themen/00103/00203/index.html?lang=en)

[46] Suter, Manuel (2006): Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action (Zurich: Center for Security Studies), p. 41.

differ considerably. Private users are interested in practical recommendations on basic protection measures, while large businesses are looking for specific consulting. The CIIP unit cannot offer a help desk for SMEs or conduct training courses for large firms, which would surpass the capabilities of any unit. Instead, the CIIP unit should find competent partners that are able to cope each with the different tasks (see Section 5). However, sometimes users may find it hard to understand why the CIIP unit – perceived as a governmental center of competence for information security – does not care more about their individual problems. Thus, in order to avoid frustrations, the CIIP unit has to define its field of responsibility carefully and communicate it clearly to the public.

It is also vital to avoid exaggerated expectations on the part of the public. The media may overstate the role of the CIIP unit and portray it as a national "cyber-cop unit", so some people might expect the CIIP unit to guarantee the security of cyberspace. For instance, by supporting banks in their fight against phishing attacks, the CIIP unit may be pushed into the spotlight, with the result that people may perceive the CIIP unit as responsible for combating all types of fraud. Thus, even though CIIP is a technical task, the importance of public relations aspect should not be underestimated – using different media to reach the public can enhance public awareness, but also carries the danger of exaggerated expectations.

6.3 The Two Customer Bases at a Glance

The division of the CIIP unit's audience into two customer bases distinguishes between the direct protection of critical infrastructures and tasks that are only indirectly related to CIIP. Table 2 provides an overview of the membership of the two customer bases.

Table 2: The two Customer Bases

Customer base	Closed	Open
Members	Selected operators of critical infrastructures (limited membership)	SMEs Citizens
Number	2-4 representatives of each member	Open
Trust	Strong Trust	Weak Trust
Build-up of Trust	Within the whole costumer base (regular meetings, interactive network), and in particular within each sector.	Media, internet, exhibitions - with the help of partners.

Figure based on Rytz 2007, p.10.

7 The CIIP Unit in Practice: A (Fictitious) Case Study

Having described the structure and organization of the CIIP unit in previous sections, this Section examines how the unit could work in practice using a case study to illustrate the internal and external processes that are triggered by incidents. The case study presented in the following is fictitious and represents an ideal response; the attack (a phishing attack, currently one of the most frequent types of targeted attacks) and the

reaction of the CIIP unit are described based on realistic assumptions. The phases of detection, incident response and follow-up are shown, although this case study describes only one of many possible scenarios.

7.1 Phase 1: Detection of the Attack

The case study is based on the assumption of a phishing attack on a bank that is a member of the Closed Customer Base (CCB). Because such an attack may be detected in different ways, the detection process is described in three different scenarios.

- *Scenario 1: the bank reports the attack.* In this scenario, the affected bank directly notifies the CIIP unit via its representative(s) and seeks assistance. The bank may have detected the attack either during a routine checkup or because it has investigated irregularities, or after having been notified by its clients. In this scenario, the CIIP unit is not directly involved in detection. It may verify the suspicion by asking the CERT team and the analysts of the Situation Center to investigate; otherwise, it may proceed immediately to incident response.
- *Scenario 2: a client of the bank reports the attack.* A key feature of phishing attacks is their focus on the clients of a bank as the weakest link in the chain of defense. Thus, clients are often the first to detect the attack. In scenario 2, clients who received suspicious e-mails in which they were asked to indicate their passwords contact the cyber-crime unit of the police. This unit passes that information to the CIIP unit, which analyzes the information and informs the affected bank. In this scenario, the reporting of incidents by citizens (via the cyber-crime unit) results in the early detection of attacks. Thus, in this scenario, the CIIP unit acts as central platform for information exchange and makes sure that important information is conveyed in a timely manner to the appropriate people.
- *Scenario 3: the attack is detected by investigations of the CIIP unit.* Both the CERT team and the analysts of the Situation Center are constantly monitoring critical indicators. In addition, they have access to a worldwide network of contacts in other CERT teams and analysts. Thus, in scenario 3, the CIIP unit detects the attack due to its own investigations or to information from various contacts. The CIIP unit should verify the findings and notify the target as soon as possible. In this scenario, the CIIP unit plays a leading part in the whole process of detection.

These three scenarios indicate the importance of the national and international network and of both customer bases. In order to detect an attack as early as possible, the CIIP unit needs to remain vigilant in every direction. The process of incident response and the follow-up is the same, however, regardless of how the attack was detected.

7.2 Phase 2: Incident Response

Since time is a crucial factor in countering attacks, the CIIP unit must initiate incident response measures promptly. Attacks are carried out at any time; therefore, the CIIP unit must be ready to respond to incidents at night or over weekends. For the purposes of our example, it is supposed that the phishing-attack is detected by the bank (according to scenario 1) on a Sunday morning. In the afternoon, the bank alerts the CIIP unit via the 24/7 helpdesk.

Due to its prior close cooperation with the responsible bank staff, the CIIP unit can be sure that the alert is justified. Thus, the incident response process is initiated immediately. First of all, further damage must be avoided. The CERT team – informed by the help desk – begins to take down the redirect servers. The major redirect servers are placed in other countries; therefore, the CERT team uses its contacts with other international CERTs. Despite its well-established international contacts, taking down all redirect servers requires several days.

In the meantime, the CIIP unit tries to alleviate the consequences of the phishing attack by filtering the phishing mails. In order to set up such filters, contacts in the telecommunication sector are activated. Since the scenario of phishing attacks has recently been discussed in workshops and was part of an exercise, the partners of the telecommunication sector are familiar to the problem. In close collaboration with the CERT team, the filters are installed only a few hours after the detection of the attack.

From the start of the incident response phase, the Situation Center keeps the affected bank informed about all measures taken. With the consent of the target, it also informs the other members of the financial sector about the nature of the phishing attack in order to allow them to take precautions. In addition, a staff member of the Situation Center briefs the public on phishing in a news broadcast on Sunday evening, so that people who read their e-mails on Monday morning will not be taken in by the phishing attack.

The incident response phase ends three days later, when the CERT team reports that due to the close collaboration with a CERT team in another country, the major redirect server has been taken down. The immediate threat of the attack is now eliminated and the follow-up phase starts.

7.3 Phase 3: Follow-up Treatments

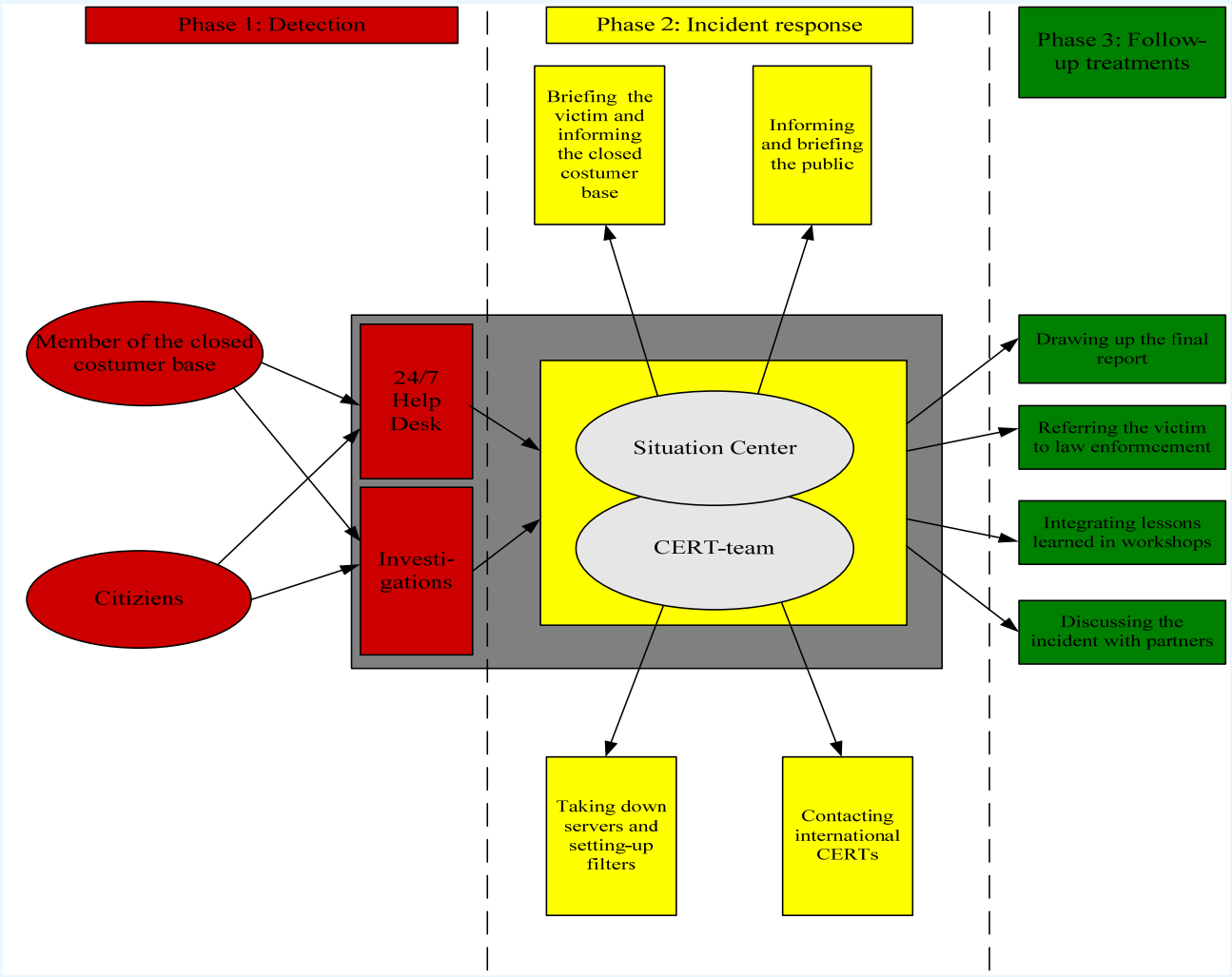
Learning from incidents is a key element of future protection measures. In order to gain insights into future trends, the CERT team analyzes the technical characteristics of the attack and discusses the attack with national and international experts. Meanwhile, the analysts of the Situation Center draw up a final report of the incident in cooperation with the affected bank. Again, with the consent of the target, all lessons learned are made available to other members of the Closed Customer Base.

For the target, the most important follow-up treatment is the prosecution of the perpetrators of the attack. Since the bank may lack experience or resources for the prosecution of Internet frauds, it appreciates the advice supplied by the CIIP unit. The CIIP unit cannot take charge of the prosecution itself, but it refers the target to the responsible authorities. Of course, the CIIP unit supplies all results of its investigations (e.g., the location of the redirect server) to the law enforcement agency.

7.4 Summary of the Proceedings

As follow-up efforts are not very time-consuming, the basic work with regard to the phishing attack may be completed within several days. However, this is only possible if the CIIP unit cooperates with various national and international partners and if the CERT team and the Situation Center share the work efficiently. The fictitious case study presented here illustrates an ideal case – in reality, delays and other problems can occur. Nevertheless, the case study offers valuable insights as to how the CIIP unit could work in practice. The proceedings described in the case study are summarized in Figure 7.

Figure 7: Proceedings of the Case Study



8 CONCLUSION

Although the necessity of CIIP is generally acknowledged, many countries have not yet established a dedicated organizational unit. Instead, responsibility is scattered across bodies in different governmental departments.[47] In addition, many private actors (ranging from the operators of CII to insurance companies) are involved. Since all of these actors are trying to shape the topic according to their interests, there is a danger of fragmentation. In order to counteract this danger, some countries have established sophisticated CIIP organizations. Unfortunately, these concepts may be less applicable to other countries, as they are often associated with high costs.

This generic framework has thus sought to offer building blocks for a national CIIP unit that is able to achieve the demanding tasks of CIIP, without consuming too many resources. The following factors are key elements of such a unit:

- With regard to the range of potential tasks, the CIIP unit should clearly define its responsibility. Its essential tasks are prevention and early warning, detection, reaction, and crisis management.
- The CIIP unit must cooperate with all relevant stakeholders of CIIP. It should be designed as a partnership involving a well-established government agency, a team of analysts from the intelligence services (Situation Center) and a center of technical expertise (CERT).
- The CIIP unit must be nationally and internationally connected. All partners should contribute their networks to the partnership. The CIIP unit can only act effectively with the help of various partners.

[47] Abele-Wigert and Dunn (2006): p. 394.

- The establishment of Public-Private Partnerships with the operators of CII, based on strong mutual trust, is essential for the success of the CIIP unit. In order to reduce vulnerabilities, information and experiences need to be shared. However, information-sharing in the area of information security is very sensitive for private firms. Thus, clear and strict rules of conduct (e.g., concerning the classification and circulation of information) is a vital for the success of any Public-Private Partnership.
- The CIIP unit should also address SMEs and private users, but cannot be responsible for the general information security of the country. As both private and public actors are interested in improving information security and raising public awareness, the CIIP unit can delegate large parts of these tasks.

These points highlight the importance of a broad network of partners. The CIIP unit acts as a platform where all involved stakeholders can get involved. By profiting from the large network and from the efforts of its partners, the CIIP unit is able to act as a center of expertise, although it focuses mainly on those tasks that are not covered by other actors. This principle of subsidiarity of all activities is pivotal to keeping the CIIP unit streamlined and cost-efficient. As a precondition for maintaining a broad network of contacts, the CIIP unit must be in continuous dialog with all partners. In particular, exchange with CII operators is essential for the success of the CIIP unit, since the work environment of these companies is constantly changing.

With regard to the ever-evolving nature of CIIP, it is important to note that this proposed framework is not presented as a single, static solution. The CIIP unit must constantly take into account the various interests of its partners, as well as to the fact that different events may demand different alliances during the problem-solving process. The case study in Section 7 is only one of many possible ways in which the CIIP unit could act. The design of the unit has to be flexible.

Finally, the proposed framework is of course not a panacea. Several problems need to be faced. First, a small CIIP unit might become dependent on a select group of individuals. As mentioned in Section 4, the CIIP unit may be staffed by less than ten people. This implies a great responsibility on the part of each staff member. In particular, the head of the CIIP unit, the leader of the Situation Center, and the leader of the CERT team are crucial actors. Since trust is often based on personal relationships, some parts of the network might be lost if the individuals in charge of them leave the CIIP unit without having carefully introduced their successors. Other difficulties are related to implementation. Building trust is a demanding task requiring a lot of time. In the meantime, it may be difficult for the CIIP unit to provide evidence of its success, as it is nearly impossible to quantify damages avoided and not incurred. Conversely, the CIIP unit might be held responsible for any incident related to information security, regardless of whether or not CII elements are affected. Thus, the CIIP unit has to define clearly its responsibilities and should communicate its work frequently to the public.

In short, implementing a CIIP policy will always be accompanied by some problems. Nevertheless, the presented generic framework showed that it is possible to form effective *and* efficient CIIP units without allocating a great deal of resources.

9 BIBILIOGRAPHY

Abele-Wigert, Isabelle and Myriam Dunn (2006), “International CIIP Handbook 2006, Vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies” (Zurich: Center for Security Studies).

Amitai, Aviram (2005): “Network Responses to Network Threats, “The Evolution into Private Cyber-Security Associations”, in Grady, Mark and Francesco Parisi (eds.), “The Law and Economics of Cyber-Security” (Cambridge: Cambridge University Press), pp. 143–92.

Amitai, Aviram and Avishalom Tor (2003), “Overcoming Impediments to Information Sharing”, Alabama Law Review, 55, pp. 231–79.

Andersson, Jan J. and Andreas Malm (2006), “Public-Private Partnerships and the Challenge of Critical Infrastructure Protection”, in Dunn, Myriam and Victor Mauer (eds.), “International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects” (Zurich: Center for Security Studies), pp. 139–68.

Branscomb, Lewis M. and Erwann O. Michel-Kerjan (2006), "Public-Private Collaboration on a National and Inaernational Scale", in Philip E. Auerswald et al. (eds.), "Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability" (Cambridge: Cambridge University Press), pp. 395–403.

Cukier, Kenneth N., Viktor Mayer-Schoenberger, and Lewis M. Branscomb (2005), "Ensuring, (and Insuring?) Critical Information Infrastructure Protection" (KSG Working Paper).

Dacy, Robert F. (2004), "Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors" (Washington, DC: United States General Accounting Office).

Dunn Myriam and Isabelle Wigert (2004), "CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries" (Zurich: Center for Security Studies).

Dunn, Myriam (2005), "A Comparative Analysis of Cybersecurity Initiatives Worldwide", paper presented at the ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 2005).

Dunn, Myriam and Victor Mauer (2006), Introduction, in Dunn, Myriam and Victor Mauer (eds.): "International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects" (Zurich: Center for Security Studies), pp.7–23.

European Network and Information Security Agency (ENISA) (2005), "Raising Awareness in Information Security: Insight and Guidance for Member States". Available at: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf.

Government Accountability Office (GAO) (2004), "Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors" (Washington DC, White House).

Grady, Mark and Francesco Parisi (eds.) (2005), "The Law and Economics of Cyber-Security" (Cambridge: Cambridge University Press).

Henauer, Marc (2004), "Critical Information Infrastructure Protection: A Swiss Approach", in: Centre for International Security Policy (CISP): EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Standards (Bern, Centre for International Security Policy).

Holderegger, Thomas (2006), "The Aspect of Early Warning in Critical Information Infrastructure Protection (CIIP)", in Dunn, Myriam and Victor Mauer (eds.), "International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects" (Zurich: Center for Security Studies), pp. 111–35.

Juster Kenneth I. and John S. Tritak (2002), "Critical Infrastructure Assurance: A Conceptual Overview", in Joint Economic Committee, United States Congress, "Security in the Information Age: New Challenges, New Strategies" (Washington, DC: White House).

Killcrece, Georgia et al. (2003), "State of the Practice of Computer Security Incident Response Teams (CSIRTs)" (Pittsburgh: Pittsburgh University Press).

Personick, Stuart D. and Cynthia A. Patterson (eds.) (2003), "Critical Information Infrastructure Protection and the Law: An Overview of Key Issues" (Washington DC: National Academic Press).

Poulsen, Kevin (2005), "U.S. Info-sharing Called a Flop", in "Security Focus", 11 February 2005. Available at: http://www.securityfocus.com/news/10481.

President's Commission on Critical Infrastructure Protection (PCCIP) (1997): Critical Foundations: Protecting America's Infrastructures (Washington DC: White House).

Prieto, Daniel B. (2006), "Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects", in Philip E. Auerswald et al. (eds.), "Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability" (Cambridge: Cambridge University Press), pp. 404–28.

Rytz, Ruedi (2007), "Reporting and Analysis Centre for Information Assurance MELANI", presentation given at the International Telecommunication Union (ITU), February 2007.

Schechter, Stuart E. and Michael D. Smith (2004), "How Much Security is Enough to Stop a Thief? The Economics of Outsider Theft via Computer Systems and Networks" (Cambridge: Cambridge University Press).

Suter, Manuel (2006), “Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action” (Zurich, Center for Security Studies).

Suter, Manuel (forthcoming), “Improving Information Security in Companies: How to Meet the Need for Threat Information”, in Myriam Dunn, Victor Mauer, and Felicia S. Krishna-Hensel (eds.), “Power and Security in the Information Age: Investigating the Role of the State in Cyberspace” (Ashgate).

United States Government Accountability Office (GAO) (2004), “Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors” (Washington, DC: United States Government Accountability Office).

United States General Accountability Office (GAO) (2001), “Information Sharing: Practices That Can Benefit Critical Infrastructure Protection” (Washington, DC: United States Government Accountability Office).

West Brown, Moira J. et al. (2003), “Handbook for Computer Security Incident Response Teams (CSIRTs)” (Pittsburgh: Pittsburgh University Press).