C-SAW: Critical Information Infrastructure Protection through Simplification

Ian Ellefsen and Sebastiaan von Solms

Academy for Information Technology, University of Johannesburg,
Cnr Kingsway and University Road, Auckland Park, South Africa, 2006
iellefsen@uj.ac.za, basievs@uj.ac.za

Abstract. The importance of Critical Information Infrastructure Protection (CIIP) cannot be overlooked, as many critical systems utilise information infrastructures in order to operate. However, should these information infrastructures be targeted by cyber attacks, it would severely affect the effectiveness of many of these critical systems. Attacks on information infrastructures are not be limited to a single geographic location, all nations suffer from a collective vulnerability through interconnection, and as such nobody is immune to cyber attacks. Many nations have created internal structures to manage and react to cyber attacks on their information infrastructure. However, these structures might not always be suitable to deploy in areas where there is no CIIP mechanisms in place. In this paper we aim to present a model for a CIIP structure that will provide protection for critical information infrastructures in a manner that is cost-effective and focused on the gradual, effective deployment of a CIIP structure.

Keywords: Critical Information Infrastructure Protection, CIIP, C-SAW.

1 Introduction

Critical Information Infrastructure Protection (CIIP) is of primary concern for all nations. Many critical systems rely on large-scale interconnected networks in order to function. However, if these networks were to be attacked, many of these critical systems could be disrupted, or prevented from operating. This would cause widespread financial and economic devastation, and there is even the possibility for loss of life.

There are many different CIIP models that have been created. CIIP structures, such as Computer Security Incident Response Teams (CSIRTs) [8, 11] provide a well-understood platform for providing CIIP.

The implementation of CIIP models in developing nations is an area of concern. Many developing nations are investing in information infrastructures, but they do not have CIIP structures in place to deal with the expanding infrastructure.

CIIP structures are widely diverse, yet they all subscribe to a simple underlying philosophy; to provide support services for computer security-related incidents [2]. Generally these models are tightly coupled, and can be expensive to implement [5], which would limit their initial effectiveness in developing nations.

In this paper we aim to discuss a model for providing CIIP through an analysis and simplification of the services required to create a CIIP structure. Firstly, we will begin our discussion with an introduction into CIIP. We will then present a high-level, conceptual model of current protection structures, and then present a number of drawbacks of this model specific to the developing world. Finally, we will then present the Community-oriented Security, Advisory, and Warning (C-SAW) Team that aims to address these drawbacks, and provide a platform for the creation of a mature CIIP structure. We will then discuss future work, and finally present our conclusions.

2 Critical Information Infrastructure Protection (CIIP)

A major area of focus is that of Critical Information Infrastructure Protection (CIIP). This is particularly true as the number of cyber attacks are on the increase [1]. The attacks on Georgia [9], Estonia [7], and the more recent attacks on Google [3], demonstrate the ability of cyber criminals to attack high-profile targets. However, CIIP is instrumental in negating the effects of cyber attack and as such it should be at the heart of all Information Technology policies, and governance procedures.

CIIP policies cannot only be concerned with local cyber events as the nature of interconnected networks, such as the Internet, increases the risk of a wide reaching cyber attack. Global reaching cyber attacks, such as those directed against the Domain Name System (DNS) root servers in 2002 and 2007 [6, 10], would have had worldwide effects had they been successful. This highlights an important fact; due to the nature of the Internet the world suffers from a level of vulnerability through the global interconnection of systems. As such, a cyber attack targeted at one system can affect many other systems.

Many different CIIP structure have been implemented to try to mitigate the effects of a cyber attack on national information infrastructures and critical systems. In the following sections we will discuss protection structures that are used to provide CIIP. We will then present a generalised structure in order to remove the complexities and isolate the core functionally of the many CIIP models that exist.

3 Protection Structures

There are many forms of CIIP protection structures that have been developed. Each country that implements a CIIP structure will tailor it to their environment, their procedures, and policies. In order to eliminate the eccentricities of each unique CIIP structure, we will discuss a generalised Computer Security Incident Response Team (CSIRT) structure. The aim of this approach is to isolate the core functionality that is required for a CSIRT.

CSIRTs are primarily concerned with providing protection for an assigned constituency [11]. A constituency is defined as being the group of individuals, organisations, or governmental entities for which the CSIRT is responsible. The

services and structure of a CSIRT will largely depend on its constituency, and the level of protection it should provide.

The definition of a CSIRT is somewhat open-ended; however a CSIRT can be defined as a group that responds to cyber security incidents which threatens its constituency [2, 8]. A further definition of a CSIRT is a group that provides computer security incident response services to its constituency [11]. Although the description of a CSIRT can be vague and dependent on its operating environment, there are descriptions of baseline capabilities for a CSIRT available [4] which allows the core functionally of a CSIRT to be identified.

Although a CSIRT structure can exist in many forms, a generic model can be derived. CSIRT structures can be defined in terms of several different layers, namely, the national coordination layer, the regional layer, and a number of specialisation sub-layers. However, the names given to these layers are dependent on the implementation of the CSIRT. A highly conceptual model of a CSIRT structure can be seen in Fig. 1. It is important to point out that international cooperation and participation is vital to the functioning of any CSIRT. A complete CIIP solution is provided through interaction between all the layers of a CSIRT hierarchy. CSIRTs provide a vital CIIP function, however they do have a number of drawbacks that we will outline in the following section.

Fig. 1. This figure demonstrates the high-level structure of a CSIRT. An important aspect of a CSIRT structure is the international relationships between CSIRTs. This allows for a high level of international cooperation and communication.

3.1 Drawbacks

The setup of a CSIRT structure has a number of drawbacks, which may prevent a developing nation from implementing an effective CIIP solution. Most importantly

CSIRTs are expensive [5]. CSIRTs require investment in two main areas, personnel, and technology.

Personnel who operate a CSIRT must be highly trained and highly competent. For developing nations this could introduce a major hurdle, as an inadequately staffed CSIRT will not operate effectively. Together with personnel, CSIRTs require a large investment in technology to operate effectively, however without the supporting technology, a CSIRT cannot adequately service its constituency.

A CSIRT structure may also be complex to implement "out-of-the-box", and investment would have to be made to contract expert knowledge to get a CSIRT structure operational.

Nevertheless, the drawbacks presented above do not outweigh the benefits of a CSIRT; however these constraints have to be addressed in order to create an effective CIIP structure. In the following section we will discuss our model for providing CIIP in which we aim to eliminate the need to make a large initial investment in the setup of a CIIP structure, while still providing effective and comprehensive protection.

4 Community-oriented Security, Advisory and Warning Team

The Community-oriented Security, Advisory and Warning (C-SAW) Team model aims to provide a simplified approach to the construction of a CIIP solution. The C-SAW model will rely on the implementation of a number of C-SAW Teams, which will be designed to be deployed and become operational quickly, with a low cost overhead.

As discussed in the previous sections, a full CSIRT structure may be too expensive to set up and maintain, both in terms of personnel and technology costs. Furthermore, facilities and services provided by a CSIRT structure may be too expensive for an initial CIIP deployment; this would detract from the primary goal of a CIIP structure, which is to provide support and protection for critical information infrastructures.

In the following sections, we will discuss the construction of a C-SAW structure by attempting to identify the core services and facilities through a process of simplification. We will then discuss the possible construction of a C-SAW structure.

4.1 Simplification of Services

To identify the CIIP elements required for a C-SAW Team, we will attempt to simplify current CSIRT structures to determine what services a C-SAW Team would be required to provide.

Traditional CSIRTs provide many different services, aimed at providing a holistic approach to CIIP. These services fall into a number of different categories, namely Reactive Services, Proactive Services, and Security Quality Management Services [11].

A CSIRT structure must provide incident handling services [11], which is a mechanism for providing support for computer security incidents. This is a fundamental requirement of any CIIP structure, and will define the core of any service

that is provided to the constituency. Therefore C-SAW Teams will have to provide such a service.

Many of the other services a CSIRT provides can be seen as "icing on the cake" for a CIIP structure. These services are not essential and therefore not initially required. These services could be introduced at a later stage to improve the service offerings.

At a minimum, any CIIP structures must provide these incident handling services. Services such as vulnerability and artefact handling can be beneficial to the overall service offering which a C-SAW Team could provide, but are not essential to the overall operation.

Simplification of the overall service offerings of a C-SAW Team will produce a solution that allows for a high-level of cost effectiveness. However, cost effectiveness has to be balanced with a level of quality of service. Incident handling alone will not provide adequate levels of service. In order to complement the incident handling services of a C-SAW Team, Vulnerability Management could be integrated to supplement the service offerings of a C-SAW Team, and thus increase its overall effectiveness.

To provide a good service quality to cost ratio, C-SAW Teams will aim to initially provide both Incident Handling, and Vulnerability Management services. This should be considered the bare minimum service level for a C-SAW Team. The identification of these two services types will become clear in the sections to follow.

In the following sections we will discuss the construction of a C-SAW Team, with regard to the services identified in the above section.

4.2 Construction

The construction of a C-SAW structure should be carefully considered, as this will determine the overall effectiveness of the particular solution. Ideally, a C-SAW Team should be able to support a number of attributes through its construction; we will discuss these attributes in this section.

In order to provide effective CIIP, the construction of a C-SAW Team will be analogous to that of a "user group", which is a common concept in technology circles, however the overall construction will the more formal in nature. A national CIIP structure could be constructed by creating a number of independent C-SAW Teams. These teams would provide computer security advice and expertise to a community of users.

For ease of the following discussion, a community will be defined as being a group of geographically related computer users, which are personal, commercial, or governmental in nature, and have a vested interest in computer security. The primary goal of a C-SAW Team will be to provide computer security advice and expertise to an assigned community.

There are a number of design goals that must be considered for the construction of a C-SAW structure. These goals will allow for a concrete definition of how a C-SAW Team will operate in relation to both its environment and to other C-SAW Teams. These goals are:

- Community Oriented
- Autonomous
- Geographically Independent

Each of these aspects of an individual C-SAW Team is important to define the overall operation of such a structure. Each of these goals will be discussed below.

4.2.1 Community Participation

A key aspect of the construction of a C-SAW Team is that of community participation, this will allow C-SAW Teams to provide effective and focused computer security advice and response. A C-SAW Team will be designed to provide computer security advice and response to a predefined community. The concept of a C-SAW community is analogous to that of a constituency in a CSIRT structure; however a C-SAW Team will rely heavily on participation from the community in order to provide an adequate level of service.

The community will not be responsible for the day-to-day operation of a C-SAW Team; it will only provide an auxiliary support function. Community support and participation will allow security information to be distributed and discussed in an efficient manner. Members of the community can use the support functions provided by the C-SAW Team and the greater community, to facilitate the transfer of knowledge and to encourage the sharing of information. For instance, if a community member is experiencing a computer security-related problem, advice and assistance could be gleaned from the C-SAW Team and the community at large, this would allow problems to be identified and corrected quickly and efficiently.

Community interaction will be vital to the success of a C-SAW Team in terms of the active role the community will play in the wider education of other community members. Education of community members should be at the heart of all C-SAW services, especially in developing nations where computer security education is not widely undertaken.

Together with providing a support function, the success of a C-SAW Team will rely heavily on community participation. In the initial stages, a C-SAW Team will rely on the community in order to provide awareness, and to build a trusted base for the distribution of computer security advice and awareness. Without this initial community support and participation, a C-SAW Team will struggle to provide an adequate service. Community participation is therefore essential to the success of a C-SAW Team as an effective CIIP structure. In the following section we will discuss the autonomy of a C-SAW Team; this will allow a C-SAW Team to effectively operate without having to rely on external CIIP structures, and external communication channels.

4.2.2 Autonomous

The concept of autonomy plays an important role in the construction of a C-SAW Team. It refers to the notion that a C-SAW Team is able to function independently, and without the assistance of a controlling organisation. This concept will allow a C-SAW Team to serve its allocated community, regardless of the state of other CIIP structures.

Although C-SAW Teams would normally operate through cooperation with other C-SAW Teams, the ability to operate autonomously would allow C-SAW Teams to

operate regardless of the underlying communication medium. This is especially important in developing nations where critical systems, such as electricity, and telecommunications, can be unreliable at times.

In the event of regular communication channels becoming unavailable, due to technical fault or even cyber attack, a C-SAW Team should be able to continue to operate. This will allow C-SAW Teams to service the community during periods when their services would be most required.

The ability to operate autonomously will rely on two factors, namely the technical ability of personnel, and the use of alternate communication mediums. The technical ability of personnel, especially in the spheres of information security, will allow a C-SAW Team to operate effectively, even if consultation with other CIIP structures is not possible. This will allow the C-SAW Team to provide a constant and consistent level of service to its community.

The use of alternate communication mediums will also allow a C-SAW Team to communicate effectively with its community and other CIIP structures. Reliance on a single communication medium, or underlying communication channel would prevent the C-SAW Team from operating in the event of the communication channel becoming unresponsive. By embracing and utilising alternate technologies, such as Cellular networks, WiFi connections, and Fax messages, a C-SAW Team can continually service its community, and provide many levels of redundancy in their ability to communicate effectively.

The ability for a C-SAW Team to operate autonomously, will greatly improve their ability to service their community even in the event of regular communication channels becoming inoperative. In the following section we will discuss the geographic independence of individual C-SAW Teams as a mechanism to maximise their effectiveness in a national CIIP structure.

4.2.3 Geographically Independent

The notion of geographic independence is a simple one, but should be discussed to fully describe the construction of a C-SAW Team. The operation of a C-SAW Team must be constrained to a particular geographic region; this partition will depend on the country that will be implementing the CIIP structure.

Constraining a C-SAW Team to operate in a particular geographic region will serve a number of purposes. Firstly, it will allow a C-SAW Team of focus on its assigned community. Secondly, it will allow the community to identify with the C-SAW Team and lastly it will prevent overlap of services with other C-SAW Teams.

The geographic independence of C-SAW Teams will allow individual teams to effectively service their community and to focus on providing an effective response to computer security incidences. Each of the three discussed construction goals for a C-SAW Team will allow for an effective and robust CIIP structure. This structure will be highly community focused and able to effectively address the needs of the assigned community. In the following section we will discuss communication between C-SAW Teams in order to build up a net of protection.

4.3 Communication

Communication within a C-SAW structure is vitally important. The communication between a C-SAW Team and its community will facilitate the transfer of knowledge and provision of services. Equally important is that of inter- C-SAW communication; this will allow teams to communicate problems, experiences, and successes to all C-SAW Teams involved in a CIIP structure.

Due to the nature of the Internet and other information infrastructures, there has to be communication between all stakeholders in a CIIP structure. Any CIIP effort without effective communication mechanisms in place will not be able to adequately provide a sufficient level of service. This would be to the detriment of the whole CIIP effort.

When a computer security threat or incident is encountered, information must be able to spread quickly and efficiently to all parties, both within the CIIP structure, and those with mutual interests in the information infrastructure. The effective flow of information will allow for a quick and decisive response to protect information infrastructures.

Communication between C-SAW Teams and communities also is important to construct a net of protection, which will be elaborated on the in the following section.

4.4 Net of Protection

Important to the creation of a C-SAW structure, is the notion of a net of protection. This refers to a protection structure being constructed of a number of small or medium size teams, with each team providing protection for a fixed sized community. The accumulative effect of a number of teams operating in unison, will allow a number of C-SAW Teams to act together to provide a complete CIIP structure.

Computer security and cyber-events should be caught and handled by the collaborative effort of a number of C-SAW Teams. As discussed above, through the use of effective communication mechanisms, information can spread quickly through the CIIP structure. This will result in effective handling of any cyber-event.

An important aspect to the construction of a C-SAW structure is the development of the C-SAW Teams. Each C-SAW Team will progress through a number of stages in its development. In the following section we will discuss each of the stages of development for a C-SAW Team as an effective CIIP structure.

4.5 Stages of Development

The development of a C-SAW Team will be divided into a number of different stages; each stage will see a marked difference in the size of the community, the number of incidents handled, and number of services offered by the C-SAW Team. The three stages of development are: the initial stage, the intermediate stage, and finally the mature stage. The nature of the relationship between the size of the community, number of incidents, and the number of services can be seen in Fig. 2. In the following section we will discuss each of these stages, focusing on the community, number of incidents handled, and number of services offered.

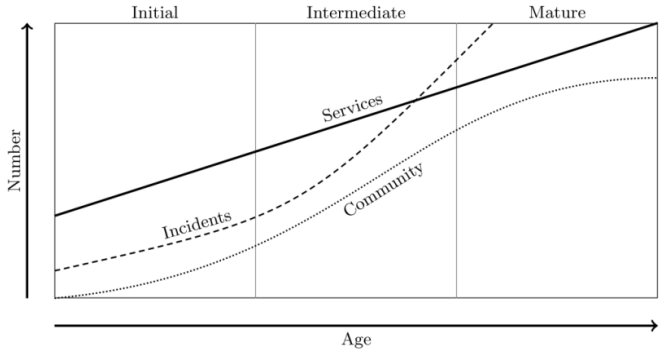

Fig. 2. This figure shows the stages of development for a C-SAW Team. The three stages of development are; the initial stage when the C-SAW Team is newly created; the intermediate stage, where the C-SAW Team has active community involvement; and the mature stage where the C-SAW Team is operating at capacity, the C-SAW Team may need to be migrated or merged to continue providing an effective service.

4.5.1 Initial Stage

The initial stages of the life of a C-SAW Team will be marked by a number of important milestones. During the initial stages, the C-SAW Team will be establishing itself, creating and deploying services to the community, and growing the size of the community.

Initially the C-SAW Team will be limited to only handling a small number of incidents; however, this will depend largely on the size of the community, and the scope of the services that will be provided. Along with growing the community base, the C-SAW Team will establish important communication links with other CIIP structures.

The number of services offered by the C-SAW Team should steadily increase during the initial stages, as the demand and requirements of the community are understood. In the following section we will discuss the intermediate stage in the life of a C-SAW Team.

4.5.2 Intermediate Stage

The intermediate stage in the life of a C-SAW Team will see rapid growth in the size of the community, the number of incidents handled, and the number of services offered. As the C-SAW Team matures, the requirements of the community will be identified, and the number and scope of services will reflect that.

The number of incidents handled will also see a marked increase. This will be due to the increasing size of the community, the increasing capacity of the infrastructure, and the increasing sophistication of computer security incidents over time. The size of the community will see the greatest growth during this period. Awareness and education of community members will contribute to this growth. The number of

services offered during this stage should also be steadily increasing to maintain service levels to the community.

The intermediate stage will be marked by the greatest levels of growth in all operating areas of the C-SAW Team. Following the intermediate stage, the mature stage will introduce the greatest number of challenges for the C-SAW Team. In the following section we will discuss the mature stage of development for the C-SAW Team.

4.5.3 Mature Stage

The mature stage will introduce the greatest number of challenges to the C-SAW Team, both in terms of the ability to function, and the ability to service the community. This will be due to reaching the operating capacity of the C-SAW Team. The growth in the number of community members will stabilise during this stage, as this will be a side effect of the C-SAW Team reaching operational capacity.

Although the number of community members will stabilise, the number of service will need to continue to increase, to allow the C-SAW Team to provide an effective level of service. Along with reaching operating capacity, the number of handled incidents will continue to increase dramatically.

The danger is that during this stage, the C-SAW Team will be unable to cope with the increasing demands on its available resources. Contingency plans will have to be put into place to ensure that the C-SAW Team will continue to operate.

Steps will have to be taken by the C-SAW Team in order to continue to provide security advice and services to the community. Either the C-SAW Team must be migrated to an alternate CIIP structure, or a C-SAW Team could be merged with other C-SAW Teams to provide a greater combined level of operational capacity.

Each of the stages of development of a C-SAW Team will bring with it its own set of challenges, specifically in terms of community, service provision, and incident handling and response. The C-SAW Team will have to continually adapt to these challenges, to allow it to provide adequate and continuing levels of service. In the following section we will discuss the question of interaction between CSIRTs and C-SAW Teams.

5 CSIRT and C-SAW Interaction

Closely related to the notion of the net of protection discussed above, is the question of the possible interaction between a CSIRT and a C-SAW structure. Although the C-SAW model is intended for deployment in an environment where an existing CIIP structure does not exist, the C-SAW model is flexible enough to be added to an environment where there is an existing CSIRT.

This would present a number of benefits to the overall CIIP structure, chief among these is the strong sense of community engagement which is key to the C-SAW Team, which is sometimes absent in a traditional CSIRT structure. A further application would be for an existing CSIRT to be used as a primary contact point for a

national CIIP initiative, and a C-SAW Team to be used as a conduit for providing accessible computer security information.

However, a new CIIP structure which relies on both CSIRT and C-SAW components could limit the initial effectiveness of the C-SAW Teams, and the CIIP structure as a whole. In the following section we will discuss areas of future research, and we will then present a conclusion to this paper.

6 Future Work

This area of CIIP offers a vast number of research opportunities; as such we plan to conduct research into the impact of a C-SAW structure as an effective CIIP solution. We further plan to expand our area of focus into the role of CIIP in the developing and newly industrialised world. This will allow us to formulate CIIP models that are appropriate for these regions. In the following section we will present a conclusion to this paper.

7 Conclusion

As discussed above, Critical Information Infrastructure Protection is of vital importance for all nations. There is an ever-pressing need to define a CIIP model that is cost-effective, easy to understand, and quick to establish. In this paper we presented the Community-oriented Security, Advisory and Warning (C-SAW) Team, which aims to satisfy the above mentioned requirements.

In order to effectively discuss the application of C-SAW Teams, their construction, and their stages of development must be fully understood. The transition from a small-scale, community-based, CIIP structure to a large-scale, broad-range, CIIP structure is a perceived strength of the C-SAW structure. This can hopefully be achieved through a careful understanding of the operational environment.

We started the discussion by introducing the need for Critical Information Infrastructure Protection in the modern world. We then presented a high-level conceptual model of existing CIIP structures. We then discussed a number of drawbacks of the current models. We then introduced the concept of C-SAW Team. We focused our discussion on the possible construction, communication, and the stages of development of such a model. We then discussed our future work in this area, and finally we presented our conclusions.

References

1. Ahamad, M.: Emerging Cyber Threats Report for 2009. Tech. rep., Georgia Tech Information Security Center (2008), http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf.
2. Brownlee, N., Guttman, E.: RFC2350: Expectations for Computer Security Incident Response. RFC (June 1998), http://www.ietf.org/rfc/rfc2350.txt.

3. Drummond, D.: A new approach to China. Electronic (January 2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
4. ENISA: Baseline capabilities for national / governmental CERTs. Tech. rep. (December 2009), http://www.enisa.europa.eu/act/cert/support/baseline-capabilities.
5. Harrison, J., Towsend, K.: An Update on WARPs. ENISA Quarterly Review, 4(4), 13-14 (December 2008), http://www.warp.gov.uk/Marketing/enisa_quarterly_12_08.pdf.
6. ICANN: Factsheet: Root server attack on 6 February 2007. Electronic (March 2007), http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf.
7. Korns, S., Kastenberg, J.: Georgia's Cyber Left Hook. Parameters 38, 60-76 (2008), http://www.carlisle.army.mil/usawc/Parameters/08winter/korns.pdf.
8. Kossakowski, K., Stikvoort, D.: A Trusted CSIRT Introducer in Europe. M&I/Stelvio, Amersfoort, The Netherlands, 2nd edition (February 2000), http://www.kossakowski.de/ti-v2.pdf.
9. Richards, J.: Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. International Affairs Review, 18(2) (2009), http://www.iar-gwu.org/node/65.
10. Vixie, P., Sneeringer, G., Schleifer, M.: Events of 21-Oct-2002. Electronic (November 2002), http://d.root-servers.org/october21.txt.
11. West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., Zajicek, M.: Handbook for Computer Security Response Teams (CSIRTs). Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 15213-3890, 2nd editon (April 2003), http://www.cert.org/archive/pdf/csirt-handbook.pdf.