FOURTH REGULAR SESSION
January 28-30, 2004
Montevideo, Uruguay

OEA/Ser.L.X/2.4
CICTE/INF.4/04
29 January 2004
Original: English

FRAMEWORK FOR ESTABLISHING AN INTER-AMERICAN CSIRT WATCH AND WARNING NETWORK

(Presented by Ambassador Margarita Escobar, Chair of the Working Group of the OAS Committee on Hemispheric Security of the OAS, held on January 29, 2004, during the Third Plenary Session)

FRAMEWORK FOR ESTABLISHING
AN INTER-AMERICAN CSIRT WATCH & WARNING NETWORK

(Presented by Ambassador Margarita Escobar, Chair of the Working Group of the OAS Committee on Hemispheric Security of the OAS, held on January 29, 2004, during the Third Plenary Session)

Objective: To develop a hemisphere-wide 24-hour per day, seven day per week network of national points of contact among Computer Security Incident Response Teams (CSIRTs) with national responsibility (National CSIRTs), in OAS member states, capable of and charged with appropriately and rapidly responding to cyber-security related crises, incidents, and threats.

As intruders use increasingly sophisticated attack tools, launch highly automated attacks that travel at Internet speed, and intentionally use attack techniques that make it difficult to understand the nature and source of the attacks, global, real-time collaboration across response teams will become increasingly important. This collaboration would:

- support rapid and accurate diagnosis of a problem;
- rapidly disseminate warnings of actual attacks across the global community;
- rapidly disseminate warnings of generic vulnerabilities across the global community;
- alert the global community to suspicious activity and support collaborations that investigate and diagnose the activity;
- provide information on mitigation and remediation strategies to combat attacks and threats; and
- minimize duplication of analysis effort across teams.

Collaboration helps to leverage the technical knowledge that exists across the teams to limit damage and ensure continued operation of critical services.

Principles:

Indigenous – The program must be operated and controlled by entities rooted in each participating nation, designated by their government.

Systemic – The system must be a multi-faceted operation requiring an aware and trained workforce, regular sharing of information regarding current threats and vulnerabilities, constant re-evaluating and implementing of best practices and appropriate interaction with public policy makers.

On-going - due to the inherent daily evolution of the Internet, any successful program must regularly be updated and maintained. Internet security will not be achieved with a one-time fix.

Accountable – The “security” in “cyber security”. Strict rules with respect to issues such as the handling of information must be understood and adhered to, or users will lose confidence and efforts to make the system more secure will be undermined and become counter-productive.

Built upon existing arrangements – There are a number of pre-existing entities in the hemisphere that provide cyber-security services to a greater or lesser extent. Any new system should build upon these pre-existing institutions to avoid duplication and encourage active participation.

Identification of Existing Organizations

There are well over a hundred organizations that use the name CERT (Computer Emergency Response Team), or CSIRT (the generic term of equivalent meaning), world-wide. Many, but not all, have some affiliation with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University where the first "CERT" was created. Even those CSIRTs associated with CERT/CC vary in their specific approaches to incident response based on a variety of factors such as consistency, geographical and technical issues, authority, services provided, and resources. In the United States, the Department of Homeland Security, National Cyber Security Division has created US-CERT, to be the "Computer Emergency Readiness Team" with national responsibility in the United States. In Canada, the Cyber Protection Division within the newly formed Public Safety and Emergency Preparedness Canada (PSEPC) fulfils a similar national responsibility role.

The Forum on Incident Response Teams (FIRST), a world-wide, voluntary association of CSIRTs, lists 79 members within the OAS Member States, of which 68 are in the US. Of the remainder, six are in Canada; two are in Brazil, and one each in Chile, Mexico, and Peru. In addition, some companies, such as ATT, Symantec, and Visa, offer CSIRT services to their customers throughout the world, and there may be other CSIRTs in the region, such as Ar-CERT in Argentina, that that are not part of the FIRST network.

Given the information gaps, conducting a CSIRT census is the essential first step towards developing a cyber-security network.

Establishing a Service Model

While there are no international agreed upon standards for what constitutes a CSIRT, there are a number of documents and efforts that can assist the process of defining a CSIRT team and on certification and accreditation of CSIRTs.

The CERT/CC has published a variety of documents that can assist in the creation of a CSIRT, including:

- *Handbook for Computer Security Incident Response Teams (CSIRTs)* provides updated guidance on generic issues to consider when forming a CSIRT;
- *State of the Practice of Computer Security Incident Response Teams*. This report includes information collected through a pilot survey of computer security incident response teams (CSIRTs), CERT/CC's own experience, discussions with and observations of other CSIRTs, and research and reviews of the current literature on incident response; and
- *Creating a Computer Security Incident Response Team: A Process for Getting Started* is a document that describes the basic requirements for creating a CSIRT.

In addition, the United States Department of Defense (US DoD) has created a program of certification and accreditation of computer network defense service providers within the US DoD. This program can be used as a starting point for establishing criteria for the accreditation of National CSIRTs.

In establishing a regional network of cooperating National CSIRTs, a minimum set of standards and services would be expected. These would include:

- designation of responsibility by the National CSIRT's government;
- agreement to principles of information sharing among the cooperating teams;
- responsibility for receiving information from other National CSIRTs and disseminating that information to appropriate entities within the country;
- authorization to disseminate information to other National CSIRTs; and
- provide coordination assistance to other National CSIRTs for incidents and threats.

Trust Issues

Much of the information which CSIRTs need to exchange is proprietary or otherwise sensitive and there are few good models that promote the consistent sharing of information among CSIRTs. Trust – the essential ingredient in information sharing – when it exists, has developed among individuals who know and have worked with each other, rather than institutionally, among organizations. To establish trust, clear expectations on how information exchanged will be used or disseminated must be understood and followed by all parties. Principles of information sharing stating how information can be used or disseminated must be agreed to among all of the cooperating National CSIRTs.

Vulnerability disclosure policies outline under what circumstances and to whom vulnerability information is disseminated. These policies must balance the need to disseminate actionable information to appropriate audiences with the need to minimize the potential that intruders will obtain the information before patches or workarounds are available.

Some of the CSIRT attributes that are required to promote trust in communication and cooperation about sensitive security issues include:

- a secure infrastructure for managing sensitive information;
- the ability to communicate securely with stakeholders;
- the ability to marshal experts and decision makers;
- an infrastructure to support advance notification to select audiences;
- procedures to guard against information leakage;
- a well-known public interface for dissemination of critical information; and
- the ability to reach a large audience quickly.

Developing a regional CSIRT capability will require the development of a consensus on principles of information sharing including what information to share, with whom, and when.

Financing

CSIRT financing is not inexpensive. In addition to providing equipment and trained staff on a permanent basis, CSIRT administrators need to provide periodic technical assistance and develop regular exercises to keep their operations sharp. Member States and the Organization will have to carefully consider CSIRT funding mechanisms and may have to prioritize their coverage, or seek stable sources of outside funding.

It should be noted that in October 2002, APEC leaders called for the development of a regional 24/7 CSIRT capability by October 2003. Both APEC and the Government of Australia agreed to fund CSIRT capacity-building projects in four member economies. In their most recent report on the project, APEC officials admitted difficulties in attracting acceptable applicants and in raising adequate funds to cover the cost of the project.

Public Awareness

Government and industry support for CSIRT programs (and financing) is closely linked to public awareness of the cyber-security problem and its potential impact on highly desirable development goals. If systems in one networked economy are not adequately protected, then the networks and infrastructures of all the interconnected economies are vulnerable. Participants in a network, whether as developer, owner, operator, or individual user, must be aware of the threats to and vulnerabilities of the network and assume responsibility for protecting that network according to their position and role. The Organization, working with Member States and CSIRTS, should undertake a public awareness program regarding cyber-security and cyber-ethics that emphasizes (1) the benefits and responsibilities of using information networks; (2) safety and security best practices; and (3) the potential negative consequences resulting from the misuse of networks. There are a number of organizations and on-line sites with useful information for this purpose; the Organization should take advantage of them.

Extending the Network

Although public awareness is an essential element of this proposal, establishing a regional CSIRT capability will require developing political commitments where they may not exist. The working group should propose a draft resolution on cyber-security for approval by the Committee on Hemispheric Security and transmission to the General Assembly for their approval, which commits Member States to establish CSIRTs in their territories and to implement such other recommendations the group may make and the Committee may approve. This will harness the Member States' political will to achieve regional CSIRT coverage and provide the Organization with the institutional framework necessary to proceed. With this resolution in hand, the working group can assist individual states to develop specific plans and, assuming adequate funding, to develop capacity-building projects in the Member States. As of this moment, no state has offered to fund this project.

Course of Action

Action Item 1: Conduct a census to identify existing CSIRTS, their membership range, and the services they provide. This will allow us to identify coverage gaps, both geographically and sectorially, and will lay the groundwork for establishing a consensus set of services which member CSIRTs will offer. A notional census questionnaire is attached.

Action Item 2: Establish a consensus for a minimum set of services that all member CSIRTs will offer. This will help shape a consistent, hemisphere-wide operating doctrine and provide the key for subsequent technical assistance activities.

Action Item 3: Draft a resolution for submission to the CHS and GA calling on Member States to create CSIRTs and implement the other proposals contained in the working group report. Of the 11 non-US CSIRTs that are members of the FIRST network, six are government-run, four are private sector, and one is run by a university.

Action Item 4: Produce a Best Practices compendium based on the consensus CSIRT services and standards, consistent with similar practices in Europe and Asia. These could include standards and protocols to undertake real-time monitoring and subsequent exchange of information throughout the network, and will become the basis of subsequent technical assistance and testing protocols.

Action Item 5: Establish a system of on-going technical assistance and information exchange for CSIRTs. Some countries will need capacity-building assistance or technical assistance to create an information protection coordination capacity or to improve existing capacities in order to meet the required standards. Financing will need to be secured.

Upon completion of Action Item 1, hold an Inter-American meeting of existing CSIRT representatives to move forward on the action items and on issues of information- sharing, identification of gaps in coverage and technical assistance, interoperability, and intercommunication. Representatives of the OAS Cyber-security Working Group would attend to provide policy input where necessary, and ensure that the issues outlined in this paper are addressed. Such a meeting would also be an important step in tackling the trust issue, and, as it would be at the technical level, would not be contingent upon GA action.