Software Engineering Institute

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

John Haller
Samuel A. Merrell
Matthew J. Butkovic
Bradford J. Willke

June 2010

SPECIAL REPORT
CMU/SEI-2010-SR-009

CERT Program

Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the United States Department of Homeland Security

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2010 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Table of Contents

Acknowledgments

The authors would like to thank the Department of Homeland Security, National Cyber Security Division; Jeffrey James Bryan Carpenter, Dr. Timothy Shimeall, Robin Ruefle, and Robert Floodeen of the CERT Program for their feedback and insights on the operations of National CSIRTS; Peter McCarthy for his assistance in compiling the additional resources; and Amanda Parente for her support in editing this document.

Executive Summary

Managing cyber security through a national strategy is a necessity common to all national governments in the 21st century. Critical infrastructure in most nations, from transportation and power generation to food supply and hospitals, depends on Information and Communications Technology (ICT). The reliance on complex and constantly evolving technology is pervasive across all sectors of critical infrastructure, making it very difficult for national governments to understand and mitigate risks related to this technology. In fact, these risks are a shared responsibility that extends outward to include international perspectives. The shared responsibility within the nation includes private industry (which owns and operates much critical infrastructures), academia, and citizens.

Establishing and maintaining a computer security incident management capability can be a very valuable component to help manage this interdependence. This capability is referred to in this document as a National Computer Security Incident Response Team (National CSIRT), but it can be implemented in a variety of different organizational forms. Beyond responding to discrete computer security incidents, a robust incident management capability enhances the ability of the national government to understand and respond to cyber threats. Operating a National CSIRT – or an organization like it - is a core component of a nation's overall strategy to secure and maintain technologies vital to national security and economic vitality.

This handbook is first in the *Best Practices for National Cyber Security* series. It is designed to be introductory curricula for capacity development within nations. The intended audience includes leaders and managers in the nation who are seeking to learn more about the value proposition of National CSIRTs and an incident management capability generally. It is not intended to be a guide on the daily operation of a National CSIRT, but as informative materials on how National CSIRTs support a national cyber security strategy and the first steps towards building this capacity.

This handbook provides principles and strategic goals to help nations develop a robust management capacity that is appropriate for the nation. It attempts to lessen the challenge many nations have in developing an incident management capability without much published guidance. Many nations attempting to develop organizations like a National CSIRT have started by attempting to copy successful CSIRT organizations that already exist. This approach can be problematic because not every nation has the same needs and resources. The operating principles and strategic goals discussed in this document enhance the ability of governments to manage cyber security risks and focus their efforts.

Strategic goals are essential design requirements and imperatives. They serve as fundamental elements of an incident management capability and are meant to provide clarity and direction. This document proposes four strategic goals as they relate to a national computer security incident management capability. They are

1. Plan and establish a centralized computer security incident management capability (National CSIRT)
2. Establish awareness
3. Manage cyber incidents
4. Support the national cyber security strategy

There is a common need to resist, reduce, and fight cyber threats and respond to attacks. National CSIRTs provide a domestically-focused, internationally-amplified operational response to those cyber incidents that destabilize the interdependent nature of global telecommunications, data services, supply chains, and critical infrastructure. We hope as a sponsor of a National CSIRT or similar capability, you will see these benefits and encourage the government and organizational leaders in your nation to participate in a global culture of security.

Abstract

As nations recognize that their critical infrastructures have integrated sophisticated information and communications technologies (ICT) to provide greater efficiency and reliability, they quickly acknowledge the need to effectively manage risk arising from the use of these technologies. Establishing a national computer security incident management capability can be an important step in managing that risk. In this document, this capability is referred to as a National Computer Security Incident Response Team (National CSIRT), although the specific organizational form may vary among nations. The challenge that nations face when working to strengthen incident management is the lack of information that provides guidance for establishing a capacity appropriate to the nation, understanding how it supports national cyber security, and managing the national incident management capability. This document - first in the *Best Practices for National Cyber Security* Series - provides insight that interested organizations and governments can use to begin to develop a national incident management capability. The document explains the need for national incident management and provides strategic goals, enabling goals, and additional resources pertaining to the establishment of National CSIRTs and organizations like them.

1 Introduction

Nations are increasingly dependent on complex systems and information technology. In many cases, Information and Communication Technologies (ICT) that are vital to national and economic security are subject to disruption from a number of causes, either originating from within the nation or outside its borders. The leaders of government and private industry organizations are increasingly confronted with uncertainty about cyber risk and vulnerabilities. This uncertainty stems from the complexity and interconnectivity of evolving technology used to support critical systems. Ensuring security and economic vitality increasingly means that nations must manage cyber security in accordance with their own economic, social, and political considerations.

Implicit in a strategy for cyber security is establishing a national computer security incident management capability. Often this capability may take the form of one or more National Computer Security Incident Response Teams (National CSIRTs). National CSIRTs are typically hosted by one or more sponsoring organizations, which build and manage cyber incident management assets. Organizations such as the National CSIRT provide value in several ways. A National CSIRT coordinates incident management and facilitates an understanding of cyber security issues for the national community. A National CSIRT provides the specific technical competence to respond to cyber incidents that are of national interest. In this primary role the National CSIRT fills a planned response function, providing solutions to urgent cyber problems. The ability of National CSIRTs and similar organizations to identify cyber security problems and threats, and disseminate this information, also helps industry and government secure current and future systems.

Beyond the capacity to react to discrete events and disseminate specific threat information, National CSIRTs can enhance the ability of national government departments to fulfill their unique roles. Most government functional areas are touched by information technology in some way. Law enforcement and the judiciary are increasingly concerned by the global movement of criminals to the virtual world to commit crimes ranging from child exploitation to financial fraud. The world's defense services rely on advanced information technology-based systems for their capabilities. And key services relating to human security, such as food, water, and electricity supply chains depend on reliable technology. A National CSIRT can enhance the government's ability to meet core responsibilities while respecting their citizens' privacy and human rights, and upholding national values of openness and pluralism.

National CSIRTs can also act as a focal point for a national discussion on cyber security. Contemporary cyber security poses new and unique social, legal, and organizational challenges. This is the case for a variety of reasons. The global interconnectedness of computer networks, the anonymity of online actors, and the rapid exploitation of cyber security vulnerabilities mean that the actions of individuals – often located outside national borders – can have serious and magnified effects on vital national systems. Meanwhile governments are limited by the jurisdictional reach of their laws and the physical limits of their borders. The National CSIRT can catalyze a thoughtful discussion on these issues, engaging authorities in the fields of education, law, and governance – among others – to help create solutions that are in keeping with national character and traditions.

Finally, building a national computer security incident management capability can help foster international cooperation on cyber security. National CSIRTs provide a domestically-focused, operational response to those cyber incidents that destabilize modern telecommunications, data services, supply chains, critical infrastructure, banking, and financial services. Collaboration with peer organizations both regionally and globally can enhance this capability and help leaders better understand the current state of the global cyber threat. There is a common global interest in securing information and information systems, and in mitigating risk. To the extent that they cooperate on cyber security issues, national governments help make the world more secure and prosperous for their citizens.

The challenge for nations wanting to develop an incident management capability is that there is little published guidance available in this area. Typically nations model nascent capabilities on the National CSIRTs or other CSIRTs which have already been operating in other nations. The problem with this approach is that the organizations that already exist are in some measure products of the historical, political, or other circumstances in those countries. One nation's solution to cyber security management may not be appropriate for another nation. To date, the published guidance on how to systematically build a cyber security and incident management capability has been in its infancy. This *Handbook Series* begins to remedy this.

1.1 Intended Audience

The primary audience for this document consists of those sponsoring the development of a national computer security incident management capability. Since the most typical organizational form for such a capability is the National CSIRT, this document will discuss the considerations and goals inherent in standing up one or more National CSIRTs. While this document focuses on the National CSIRT, there may be other organizational forms that are suitable for an incident management capability. Alternatively, some nations may find it advantageous to house this capability across several organizations. It is hoped that the principles and recommendations in this document are useful even to nations that do not choose the specific National CSIRT organizational form.

1.2 About the Best Practices for National Cyber Security Handbook Series

The *Best Practices for National Cyber Security* series of handbooks is designed for leaders and key stakeholders in critical infrastructure protection, government, and industry, or anyone interested in cyber security policy and management. It is intended to be foundational material for individuals and organizations working to develop a strategy for national cyber security management. Each handbook in the series will provide a tailored message. In addition to this initial document, the series will address such topics as:

- Managing CSIRTs with National Responsibility
- Public Private Partnerships in Cyber Security
- Building a Culture of Cyber Security
- National Policy Frameworks for Cyber Security
- Managing and Participating in Cyber Security Exercises
- Cyber Security Assessment and Evaluation

The subject matter presented in the other handbooks is formatted similarly, but emphasizes a unique function of national cyber security and goes into more depth.

1.3 How to Read This Handbook

This document is structured to serve as a strategic education on the building of a computer security incident management capability. Because of the breadth of this topic, the focus here is on the creation of a National CSIRT. The material is intended to outline the stakeholders, constraints, and goals for National CSIRTs, to raise awareness of the need for this type of capability, and to frame this capability in the national strategy.

While the focus is on National CSIRTs specifically, the guidelines herein are meant to help national leaders generally, regardless of the specific organizational form chosen to handle incident management.

The next section, *Setting the Context: National Cyber Security*, includes information about National CSIRTs as part of a larger national approach to cyber security. The section specifically discusses the importance of a national strategy, the context of a national cyber security policy framework, and an overview of key stakeholders in national cyber security as they relate to National CSIRTs. The special role of National CSIRTs, and how they differ from organizational CSIRTs, is also discussed.

The third section, *Strategic Goals and Enabling Goals for Incident Management Capability*, introduces a hierarchy of goals for ensuring alignment between the National CSIRT and national cyber security strategy. *Strategic goals* outline the long term imperatives for a national computer security incident management capability, while the *Enabling Goals* highlight the necessary steps to building an operational National CSIRT capacity. These goals and practices will be expanded in other handbooks in this series.

Section four offers a case study of national incident management in the United States. It includes an explanation of how the U.S. Department of Homeland Security operates the United States Computer Emergency Readiness Team (US-CERT) as its National CSIRT. The handbook is concluded in section five.

2 Setting the Context: National Cyber Security

Ensuring national security and economic vitality requires recognizing that not all risk is owned and mitigated by a nation's government. The national and local government and its various branches, critical infrastructure owners and operators, academia, and citizens all share this responsibility. New and emerging risks must be effectively identified, analyzed, and mitigated to ensure the safety and security of daily life for citizens. These risk management activities may involve ensuring continuity of government, safeguarding the generation of electricity, emergency response services, or ensuring a reliable supply chain, among others. Each of these relies heavily on information technology in a modern economy. National leaders increasingly realize that the security of information and information technology is a national security interest and should be codified in laws and national strategy. Chief among the strategies for enhancing this security are specific operational capabilities, such as the incident management activities typically performed by a National CSIRT.

2.1 The Importance of a National Strategy for Cyber Security

Building a national strategy for cyber security is ideally the first step in establishing a national cyber security program. A national policy framework for cyber security should explain the importance of cyber security, help stakeholders understand how their activities may affect security, and set the goals and priorities in this area of security. The strategy can establish the authority for the various organizations and stakeholders to execute their respective responsibilities. The national strategy can also serve as a backdrop for the creation of laws that relate to cyber security; for instance in the areas of computer crime, the protection of intellectual property, and privacy. Finally the national strategy should reconcile the need for security with the need to honor citizens' rights and the nation's cultural values and norms.

The strategy should also articulate the need for specific operational capabilities, such as national incident management. The goals that a nation identifies and promotes through its strategy align the program to a consistent vision (i.e., manage cyber risk) and establish a clear direction for the efforts of the program (i.e., build and operate the National CSIRT). The national strategy should stress the benefits of a culture of cyber security, integrate security fundamentals (such as raising awareness), and emphasize cooperative relationships among national stakeholders. The strategy should also include sufficient detail to allow stakeholders to internalize the stated goals and evaluate progress toward achieving them. Thus, the National CSIRT should be deliberately aligned with national cyber security strategic goals to ensure that its work is performed to achieve them.

Finally, the national cyber security policy framework should encourage participation from owners and operators of critical infrastructure, clearly define the government's role in developing a culture of security, prescribe effective continuous risk management, and help facilitate information sharing with all stakeholders.

While establishing a national strategy is ideally the first step, in many cases this may not always be feasible. This might be the case because of the difficulty in getting a large number of stakeholders to agree on a strategy. Alternatively, national leaders may judge that establishing an incident management capability is a more pressing need than creating a fully integrated strategy. In such cases creating an effective strategy may occur concomitantly with building incident management capability. In any case, the sponsor or proponent of the National CSIRT should work with the government to ensure that national needs and strategy are considered throughout the process of building and managing a National CSIRT.

2.2 Key Stakeholders of National Cyber Security

Cyber security strategy has a large number of important stakeholders. This section broadly describes the roles and responsibilities of key stakeholders, and how they might contribute to a national program for managing cyber security. These roles are not unique to National CSIRT operations, but many of the stakeholders discussed here may directly interact with the National CSIRT. Moreover, the National CSIRT can enhance its role and help advance a culture of security by proactively interacting with these stakeholders.

The government has a multitude of roles and responsibilities to strengthen national cyber security. The primary role is to define the national strategy and provide the policy framework. The policy framework describes the architecture by which the national efforts are built and operated. Following that, the government has a responsibility to participate with all stakeholders in efforts to identify, analyze, and mitigate risk. This area is further divided to describe the roles and responsibilities of the various branches of government. The government also has a key role to play in the arena of international relations and cyber security, particularly in the areas of treaties relating to cyber security and the harmonization of national laws relating to cybercrime.

2.2.1 Executive Branch of the Government

The executive arm of the government is typically the sponsor of the national cyber security program. In the United States, for instance, the execution of laws – including those relating to cyber security – is constitutionally delegated to the executive branch of government. The executive area of government must ensure that the program remains viable and has appropriate resources (e.g., is authorized, staffed, funded, etc).

2.2.2 Legislative Branch of the Government

The legislative arm of government must work to provide effective laws and treaties that promote a culture of cyber security. Whether through appropriations of resources or funding, legislation that mandates execution of the national strategy, privacy or tort laws, or laws that establish criminal behaviors, the legislature must ensure that the national cyber security program has the foundation it needs to be successful.

2.2.3 The Judiciary

The nation's judiciary and legal institutions have an important role to play in a national cyber security strategy. This role relates specifically to providing clarity and consistency in areas of law that may affect cyber security. Privacy law is one of these primary areas. By working with their global counterparts, the legal community can also help to limit the ability of criminals and other malicious actors to take advantage of differences in legal jurisdictions.

2.2.4 Law Enforcement

Law enforcement must ensure that legislation related to cyber security is supported and enforced. Additionally, law enforcement can serve as an important source of intelligence about malicious activity, exploited vulnerabilities, and methods of attack. Sharing this information allows critical infrastructure owners and operators to learn from the experiences of others to improve their own cyber security practice and management. Finally, law enforcement can enhance cyber security by cooperating with their counterparts in other nations on the pursuit and apprehension of criminal actors who affect systems regardless of geographic borders.

2.2.5 Intelligence Community

The intelligence community plays an important part of watch and warning for technical infrastructure. Because they have an understanding of the deployed technologies, intelligence organizations have the ability to monitor information sources for news about the latest threats and vulnerabilities to a nation's infrastructure. This information should be distilled and provided not only to the infrastructure owners, but also to the National CSIRT, ensuring that attacks are efficiently recognized and resolved.

2.2.6 Critical Infrastructure Owners and Operators

The components of critical infrastructure depend on the nation's economic system and technological sophistication, among other factors. A general definition for critical infrastructure is:

> *Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*

Critical infrastructure owners and operators are a very important stakeholder in the nation's overall cyber security strategy. Infrastructure operators typically have an understanding of how security threats and vulnerabilities affect their sector. In addition they frequently possess knowledge about how vulnerabilities affect proprietary systems and software, such as Supervisory Control and Data Acquisition Systems (SCADA). Infrastructure operators also have the daily task of implementing the security recommendations or mandates created by the national government and other authorities. They must reconcile the need for security with the sometimes contradictory goals of efficiency and profitability.

Because of their unique position, infrastructure owners and operators frequently have very valuable information, ranging from the actual software problems and cyber attacks they may experience, to the efficacy of countermeasures or risk mitigation strategies. They are also a primary consumer of information about security vulnerabilities. Finally, because of their practical experience implementing security standards and complying with the law, owners and operators may have valuable input into the development of effective, realistic rulemaking and legislation.

2.2.7 Vendors

Vendors of information technologies and services must contribute to national cyber security through development practices and ongoing vulnerability reduction efforts. Vendors can often be the source of vulnerability information; they ensure that users have up-to-date information and technical solutions to mitigate known vulnerabilities. Ideally, vendors will participate with National CSIRTs and help extend the analytical and problem solving capabilities the National CSIRT needs to conduct incident response. Information sharing among vendors, their major customers, and the National CSIRT can create a partner relationship that continuously improves security for technologies and services.

2.2.8 Academia

Academia is important to national cyber security policy for a number of reasons. Educational institutions play a key role in developing the human capital and technical skills needed to solve complex problems, such as aspects of cyber security. Academicians conduct research that enhances the technical, legal, and policy aspects of cyber security. Finally, in many countries educational institutions have championed and hosted National CSIRTs.

2.2.9 Foreign Governments

Nation-states must take an interest in helping to prevent any cyber security attacks against their neighboring nations and allies. For a number of reasons, including economic, political, and infrastructure concerns, partnerships should be established to discuss global risk and interdependence. Allies and neighboring nations can also provide a valuable source of intelligence and promote regional cyber prevention and preparedness.

2.2.10 Citizens

Citizens rely on all stakeholders to create national security and critical infrastructure stability. The citizens of a nation have a stake in the reliable performance of a nation's strategy for cyber security, and are an inherent part of that strategy.

2.3 The Special Role of the National CSIRT

National CSIRTs and organizations like them ideally act as critical components of the national cyber security strategy. National CSIRTs first provide the capability to react to computer security incidents that are deemed to be of national importance[1]. Because they collect and analyze information about computer security incidents on a daily basis, National CSIRTs are an excellent source of lessons learned and other information that can help stakeholders mitigate risk. National CSIRTs can also help catalyze a meaningful national discussion about cyber security and awareness by interacting with private and governmental stakeholders. The following is a discussion of the special roles of a National CSIRT and the ways in which National CSIRTs are distinct from the various organizational CSIRTs in a country. Not every National CSIRT will fill these functions or do all of these tasks. However, these are the several ways that a National CSIRT can fulfill its unique role in national incident management.

2.3.1 Analyzing Computer Security Incidents to Identify Intrusion Sets

An intrusion set is defined as groups of computer security incidents that share similar actors or methods. Determining that similar actors are involved may involve a variety of analytical techniques, and is closely tied to the question of method. Determining that different attacks use the same method may involve questions of attack vector (email, spoofed web pages, etc.), similarities across samples of malware, or the routing of stolen information (through specific proxy IP addresses, for instance).

Generally, analysts group activity into different categories, such as

- criminal activity
- activity conducted by other nations
- undetermined

This information and analysis can then be submitted to other national authorities for action depending on the nation's security concerns and objectives.

2.3.2 Use of Sensitive Law Enforcement or Intelligence Information

Because of their national mission, their often close relationship with the national government, and their daily work safeguarding sensitive information, National CSIRTs may be involved in using sensitive information

[1] The question of which incidents rise to the level of national importance is covered more fully in section 3.3.1.

from national intelligence or law enforcement organizations in their analysis. The use of this type of information can amplify the National CSIRT's work, but requires strong trust relationships between the National CSIRT and the government.

2.3.3 Resource to the National Government on Cyber Security Issues

A National CSIRT can be a valuable resource to the national government on technical, policy, and legal issues relating to cyber security. It may be able to advise the government on the suitability or security of systems the government is planning to install or implement. In addition, the National CSIRT can help government organizations with technical alerts and bulletins, best practices, and other advisories.

2.3.4 Assessing National Cyber Readiness and Crisis Management

The National CSIRT can help national leaders and key stakeholders test and measure the nation's level of resilience to cyber attacks and crises. This assistance may take the form of providing the technical support and analytical methods to plan and stage exercises, or advising on the state of current cyber threats or the realism of exercises.

2.3.5 National Alert and Warning

Most of the existing National CSIRTs fulfill a national alert and warning function. This function involves alerting key national communities about problems ranging from specific software and system vulnerabilities, to evolving criminal methods, to malware threats.

2.3.6 Organizational CSIRT Capacity Building

National CSIRTs have a key role to play in the building of cyber security capacity. Specifically, National CSIRTs can help organizational CSIRTs in the nation in a variety of ways including advice, training, best practices, or in some cases staffing.

2.3.7 Trusted Point of Contact and National Coordinator

National CSIRTs frequently act as a trusted point of contact for the nation on cyber security issues. For example, national teams often handle requests from other nations or foreign organizations concerning malicious activity emanating from computers or systems within the nation. In a similar fashion, National CSIRTs frequently act as coordinators for domestic organizations attempting to resolve cyber security incidents. In this role, the National CSIRT does not typically analyze or resolve incidents itself, but rather it helps to direct organizations experiencing security incidents to information, services, or other entities that can help them.

2.3.8 Building a Cyber Security Culture

The National CSIRT can help to build a cyber security culture within the nation. Building a cyber security culture consists of many activities including awareness and education of private citizens on online risks, educating national stakeholders on the impact of virtual activities to their organizations, and the implications of their activities for cyber and information security.

3 Strategic Goals and Enabling Goals for Incident Management Capability

This section provides the strategic goals and enabling goals that should be considered when establishing a national computer security incident management capability. This capability is referred to as a National CSIRT. The information provides an overview of the considerations and hierarchy of goals that are needed to ensure support for the national cyber security strategy and to align the National CSIRT with the national strategy. The enabling goals are specific steps to meeting strategic goals. Four strategic goals are established for a National CSIRT:

1. Plan and establish a centralized computer security incident management capability (National CSIRT)
2. Establish situational awareness
3. Manage cyber incidents
4. Support the national cyber security strategy

Each of these strategic goals explains the fundamental elements of the National CSIRT and must be weighed carefully by the National CSIRT sponsor. Strategic goals are essential, long term requirements that help build the capacity to react to cyber incidents and enhance information and cyber security on a national level. Following each strategic goal are Enabling Goals. Enabling Goals help the sponsor build the capacity. They explain the more detailed considerations and activities needed to implement the strategic goals. The guidance available for each goal varies based on the maturity of the topic. Some subjects, like incident handling, have a robust history. Others, such as implementing national cyber security strategy through National CSIRTs, are still emerging disciplines.

This document is not meant to provide specific ‘how-to’ instructions. Instead, it highlights the unique requirements for building capacity in cyber incident management. Finally, each strategic goal section concludes with a listing of additional references and training resources. These sources are not exhaustive, but provide the reader with a ‘next step’ to both training and informational resources.

3.1 Strategic Goal: Plan and Establish a Centralized Computer Security Incident Management Capability (National CSIRT)

Before the first cyber security incident can be managed, the capability must itself be established in an organizational form such as a National CSIRT. Having a sole source or point of contact for computer security incidents and cyber security issues provides a number of benefits. A single organization provides stakeholders with a known source of information. A National CSIRT can also provide the government with a conduit for coherent, consistent messaging on cyber security issues. With a single National CSIRT, government departments have a source for technical information to support their individual functional areas. Finally, the National CSIRT can encourage the discussion about cyber security and facilitate international cooperation on this issue. In some nations, unique considerations may dictate that there are multiple NCISRTs, or even an incident management capability that is spread across several organizations. This can be entirely appropriate. This document provides guidance regardless of the exact organizational form.

A National CSIRT capability should be established and operated according to certain core principles. These principles help leaders make decisions in the face of limited resources and frequently complex problems. The core principles for the national management capability are:

- Technical excellence. The National CSIRT's capability should be the best that it is possible to develop given the resources available. This is important because the National CSIRT strives to be a trusted leader in the nation on computer security issues. While striving for excellence may seem an obvious point, it has certain implications for building a capacity subject to resource constraints. It implies, for instance, a preference for building one or two outstanding capabilities versus attempting to establish a range of capabilities without proper staffing or funding. The emphasis should be on technical competency.
- Trust. Almost by definition, a National CSIRT will handle information that is sensitive or potentially embarrassing to stakeholders. Trust must be earned and maintained. Properly handling and protecting confidential information is an important component to building and managing this trust.
- Resource Efficiency. Resource efficiency means using the resources that are available effectively. This consideration will be covered in more detail below, but it implies an ongoing evaluation of which threats and incidents are truly of interest to the National CSIRT's overall strategy as well as to the community it serves.
- Cooperation. The National CSIRT should cooperate as fully as possible with both national stakeholders and other National CSIRTs to exchange information and coordinate the solving of problems that are frequently very complex.

Chief to the National CSIRT's success is adequate sponsorship and resourcing. The Enabling Goals listed here are intended to help the sponsor of a national incident management capability build this capability in the most robust way possible. Consider the following enabling goals in planning and creating the national incident management capability.

3.1.1 Enabling Goal: Identify Sponsors and Hosts

The sponsor of the National CSIRT should identify other sponsors and likely hosts for the National CSIRT. Other sponsors may be able to bring additional funding and support to the National CSIRT project. Of course, a physical location – or host – for the National CSIRT must also be identified. In many countries the host has been an academic institution. Universities traditionally have been a venue for National CSIRTs because aspects of their core mission – to serve the community and conduct research and analysis of difficult problems – aligns well with the mission of a National CSIRT. However if it is hosted by a university, the National CSIRT may not have adequate resources or the authority to enforce or take action; rather it achieves its success by influencing others through its good work.

There may be a variety of institutions and government departments interested in supporting or hosting a National CSIRT. While any assistance is welcome, there may be pitfalls to receiving support from certain stakeholders. The National CSIRT should be dedicated to serving its entire community in an unbiased fashion, without favor to a particular stakeholder. Receiving sponsorship from an entity that is closely tied to a particular stakeholder or industry may limit the National CSIRT's perceived ability to service the entire community. This possibility should be examined, for example, if a specific for-profit enterprise operated a National CSIRT. In other cases, the involvement of certain sponsoring organizations may impede the willingness of key constituents to share information. Certain constituents, for instance, might be reluctant to share information if a law enforcement organization was the National CSIRT's primary sponsor. In addition, the National CSIRT host should be sufficiently financed to ensure fiscal stability for continuity of operation.

3.1.2 Enabling Goal: Determine Constraints

The sponsor should determine what constraints may act to limit building and operating a National CSIRT. Typical constraints are budget, the availability of skilled staff, and the physical infrastructure available to support National CSIRT operations. The question of constraints bears heavily on the ability of a national government to build incident management capacity, and is usually a key driver behind decisions about which specific services to offer to the community. For instance, it may not be practical or desirable to build a malware analysis or deep packet inspection capacity in the National CSIRT. Limited constraints may dictate that a more realistic approach is to build relationships with other domestic or overseas organizations that do have this capability.

Constraints relate strongly to three of the core operating principles identified above; technical excellence, trust, and resource efficiency. Technical excellence requires a clear understanding of the staffing and budget available to support certain CSIRT activities. It may dictate an emphasis on a few core services performed well, rather than attempting to provide a broad array of services. Limited constraints can also make the ability to coordinate incident management very important, rather than attempting to complete every incident management task in-house. Earning the trust of key constituents requires operational and staffing stability, as well as the ability to safeguard sensitive information – all directly impacted by resource limitations. Finally, resource efficiency requires understanding what resources are available.

3.1.3 Enabling Goal: Determine the National CSIRT Structure

Based on its function in national cyber security, a National CSIRT can operate under a range of modes including: an independent agency with limited operating partnerships, a joint operation with national telecommunications providers, or an integral part of the national military defense strategy. Therefore, a number of considerations must be identified to ensure detection and incident coordination and response are appropriately structured. The following list of structural considerations is meant to be exploratory and not comprehensive:

- What level of government directs the National CSIRT?
- Who funds the National CSIRT and who approves the budget?
- Is there an independent body that oversees the National CSIRT?
- What set of roles and responsibilities have been identified for National CSIRT operating partners?

There are several considerations that may be helpful in resolving the question of organizational form, in addition to the core principles:

- What structure would best allow the National CSIRT to alleviate potential stakeholder concerns with regard to sharing information? Do the nation's privacy laws have any implications for the best structure for a National CSIRT?
- Are there any possible organizational structures that may limit the National CSIRT's perceived ability to serve its community in an unbiased fashion?
- Are the nation's systems and infrastructure already structured in ways that would make multiple National CSIRTs beneficial in terms of information sharing or reporting relationships?

- If multiple National CSIRTs are instituted, how should they share information? Is there a risk that multiple National CSIRTs may not be able to effectively share information across infrastructure sectors? What are the transaction costs associated with having multiple organizations? How to they compare to the benefits of scale of a single National CSIRT?[2]
- Do the various possible organizational forms have any implications for staffing and managing human capital?

3.1.4 Enabling Goal: Determine the Authority of the National CSIRT

The National CSIRT proponent or sponsor should determine if the National CSIRT will have the authority to proscribe or mandate certain actions or security measures. The authority of a National CSIRT could involve mandating the reporting of security incidents, or the adoption of certain security measures, or both. In addition, the authority of a National CSIRT may differ based on whether it is addressing private citizens and industry, or government departments. It may be entirely appropriate for the National CSIRT or the sponsoring organization to maintain authority over various government departments, but to have no authority over private citizens.

These decisions will be made consistently with the nation’s law and culture. However, it is frequently the case that National CISRTs are more effective when they act in an advisory role only. Major national stakeholders are often more willing and – depending on the legal environment – more able to fully share information and discuss security vulnerabilities in a collaborative venue where the National CSIRT is not a regulatory or proscriptive body.

[2] A Note about Regional Collaboration: The sponsor of a National CSIRT may consider sharing resources and costs with neighboring nations to form a regional computer security incident management capability, essentially a “Regional CSIRT.” This may be an effective way to address the inherent problem of fulfilling many requirements with limited resources. A full examination of such an arrangement is beyond the scope of this report; however there are compromises inherent in this solution.

Because one of the primary functions of a National CSIRT is to reconcile the need to respond to global challenges with the nation’s embedded law, culture, and national structure, the ability of a regionally-based CSIRT to provide value to multiple nations may become diluted. Secondly, because cyber security is part of a nation’s overall security strategy, Regional CSIRTs may often possess information that has important national security implications. A Regional CSIRT may be limited in its ability to solicit this information from certain national stakeholders because of concerns about sharing this information in a multi-national venue. Sharing this sensitive information would require thoroughly anonymizing it. In any event, it would require a high degree of comfort and familiarity between nations - or an effective multi-national governance structure - for a regional CSIRT to be successful.

3.1.5 Enabling Goal: Determine the Services of the National CSIRT

The minimal essential function of a National CSIRT is the ability to respond to cyber security threats and incidents that are of importance to national stakeholders. The various National CSIRTs currently in existence execute a variety of functions. These functions include:

Incident Handling Services

Incident Analysis

Forensic Services

Network Monitoring Services

Malicious Code Analysis

Vulnerability Assessments

Research Services

Training/Education/Awareness

Coordinating Response

At the individual nation level these functions are limited by the constraints identified in Enabling Goal 3.1.2 (e.g., funding, staffing, physical resources). The National CSIRT sponsor organization must determine which of these activities are realistic given the constraints involved. Typically the most significant constraint is human capital (i.e., staffing). Since the National CSIRT serves as the national leader in cyber security incident management and analysis, the guiding principle for choosing particular functions should be excellence. It may be that the best way for a particular National CSIRT to fulfill its role is through close coordination with other National CISRTs that have a greater technical capability, or who may already have trusted communication channels.

3.1.6 Enabling Goal: Identify Additional Stakeholders

The sponsor of the national incident management capability should evaluate which other institutions may have input or interest in the establishment of a National CSIRT. A detailed list of the typical stakeholders in national cyber security policy appears in section two of this document. Additionally, some stakeholders may be interested in taking a more active role in the formation and operation of a National CSIRT. Typically these include;

- law enforcement
- technology vendors
- government users (government agencies and ministries, etc)
- research communities
- governance bodies

The National CSIRT should understand how the identified stakeholders complement and integrate into National CSIRT operations, and develop a plan to ensure that bi-directional communication is designed into its operations.

3.1.7 Additional Resources: For Planning and Establishing a National CSIRT

The following is a list of publicly available resources for sponsors and champions considering the establishment of a National CSIRT.

Reference materials

- CERT's Resource for National CSIRTs: http://www.cert.org/csirts/national/
- CERT listing of National CSIRTs: http://www.cert.org/csirts/national/contact.html
- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?: http://www.cert.org/csirts/csirt-staffing.html
- Resources for Computer Security Incident Response Teams (CSIRTs): http://www.cert.org/csirts/resources.html
- Forum of International Response and Security Teams: http://www.first.org
- Forums of Incident Response and Security Teams (FIRST) Best Practice Guide: http://www.first.org/resources/guides/#bp21
- ENISA: Support for CERTs / CSIRTs: http://www.enisa.europa.eu/act/cert/support
- ENISA: Baseline capabilities for National CSIRTs: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

Training resources

- CERT Overview of Creating and Managing CSIRTs: http://www.sei.cmu.edu/training/p68.cfm
- CERT Creating a Computer Security Incident Response Team (CSIRT): http://www.sei.cmu.edu/training/p25.cfm
- CERT Managing Computer Security Incident Response Teams (CSIRTs): http://www.sei.cmu.edu/training/p28.cfm

3.2 Strategic Goal: Establish Shared Situational Awareness

The essential function of a National CSIRT is the ability to manage cyber security threats and incidents that are of importance to national stakeholders. Excellence in incident management helps the National CSIRT to build relationships with stakeholders and achieve other strategic objectives, such as supporting the national cyber security strategy. The first step in managing incidents is establishing an understanding or awareness of who the National CSIRT's major constituents are, what types of systems they employ (Information and Communications Technology), and what types of incidents they are experiencing. This general understanding of the environment is typically referred to as shared situational awareness.

The most able staff and the best technical infrastructure are wasted if the community is unwilling to inform the National CSIRT about incidents. Therefore, the first enabling goal focuses on this issue.

3.2.1 Enabling Goal: Establish and Maintain Trust Relationships

National CSIRTs collect sensitive information about national constituents' problems, concerns, and vulnerabilities. They frequently use this information to derive lessons learned and publish informational reports, a process which carries the risk of revealing too much information if performed carelessly. National CSIRTs also disseminate general information to stakeholders about threats, vulnerabilities, and best practices. Building trusted relationships with stakeholders is essential to facilitating this two-way information exchange. Without the confidence of knowing that sensitive information will be adequately protected and compartmentalized, stakeholders will be unwilling to share their sensitive information, crucial to the National CSIRT. Stated plainly, it is difficult to manage security incidents when the victims are unwilling to tell the National CSIRT about them.

By establishing relationships and partnerships with owners and operators of national critical infrastructure and other key constituents, the National CSIRT gains access to information crucial to its operations. These relationships and partnerships are directly with the National CSIRT and among constituents. The National CSIRT may act as a trusted communications channel between key constituents.

Ensuring the confidentiality of stakeholder information is an information security problem. It requires information security risk assessments at the National CSIRT level and implementation of the resulting recommendations. Policies to strengthen information security range from properly vetting employees to employee Non-Disclosure Agreements (NDAs) and similar legal devices, which make maintaining confidentiality a condition of employment. Classification levels for information are another basic way to ensure that access to information is limited to persons who need it to perform their job. Regardless of the specific security measures and policies, the National CSIRT should proactively address stakeholder concerns in this area and be as transparent as possible about the security steps taken. A fuller discussion of policies to facilitate information sharing and security in a National CSIRT environment will appear later in this series.

3.2.2 Enabling Goal: Coordinate Information Sharing between Domestic Constituents

One of the most important factors in establishing a national capability is to facilitate reliable and effective information sharing. A key role for a National CSIRT is to obtain incident information from the community and to disseminate timely and relevant response information back to the community. This type of information generally includes the following:

- incoming information about security incidents, collected through a variety of means
- security bulletins, awareness information on cyber threats and vulnerabilities
- general, specific, and urgent cyber warnings and alerts (technical and non-technical)
- best practices to prevent cyber security problems, events, and incidents
- general National CSIRT information (e.g., organizational chart, sponsorship, services provided by the National CSIRT, contact number/email address, etc.)
- resources and reference materials (e.g., security tools, partner organizations)

The information that the National CSIRT collects can be used to reduce risk by providing support to organizations that have been attacked. This support may take the form of direct technical support or it may involve working with third parties to find remedies and workarounds, or raising awareness of the general and private industry. A key part of information sharing is that sensitive information from constituents may be shared with other constituents only after being anonymized during the analysis process and in accordance with the National CSIRT's policies.

Anonymization requires sensitivity to specific circumstances, either involving computer security incidents themselves or the major constituents. For instance, a publicized incident report may redact the names of the victims or the constituent company involved. However, if it involves a notable incident discussed in the press, it may fail at actually protecting confidences. A basic principle of protecting information is receiving the approval of the parties involved before releasing information or publicizing reports.

A key component of information sharing is maintaining tools, techniques, and methods that enable the National CSIRT to communicate with its community. Examples of these can include the following:

- a website for communicating and disseminating information – both general (publicly accessible) and sensitive (secure portal requiring authentication) between the CSIRT and its community
- mailing lists, newsletters, trends and analysis reports
- implementation of secure information networks for CSIRT operations

3.2.3 Enabling Goal: Integrate Risk Information from the Community

National CSIRTs benefit from open, shared information from private industry, academia, and government. When organizations conduct thorough risk assessments and share the results with the National CSIRT, situational awareness increases. Risk information from the community can help the National CSIRT understand the effect that security vulnerabilities and system problems might have on important assets and infrastructure, helping the National CSIRT to focus and refine its incident management process.

In its operational role of responding to incidents, a National CSIRT is a key contributor to situational awareness. By analyzing trends in the incidents being managed, the National CSIRT learns about the status of cyber security within the community it serves. The National CSIRT uses this knowledge and its own perspective on problems to produce a credible, realistic picture of national situational awareness. This helps the National CSIRT to identify proactive defense strategies, as well as needed improvements in practices and behaviors within the community.

3.3 Enabling Goal: Collect Information about Computer Security Incidents

A National CSIRT must be able to collect information about computer security incidents and events, receiving reports about suspected or confirmed incidents that require coordination or response. National CSIRTs collect information about incidents through two primary means; the trusted relationships they build and the technical infrastructure required to process incoming reports. While incident reporting is frequently voluntary and facilitated by trust, in some cases it may be mandated.

A National CSIRT receives reports of computer security incidents through a variety of technical means, such as a 24/7 hotline or web portal. Web portals may be accessible from any computer for the general public or may be a secure web portal for the exchange of sensitive information. Capturing reports about computer security incidents requires the community to detect, identify, and track anomalous activity, employing both technical and non-technical methods. Anomalous activity is defined as activity that deviates from some establish norm of system operation. In many cases, collecting computer security incident information may first require educating communities about detecting this activity.

3.4 Strategic Goal: Manage Incidents

A National CSIRT, acting as a trusted, national cyber security focal point, is uniquely situated to manage incidents of national concern. To accomplish this, many National CSIRTs establish certain active capabilities, such as incident response and containment, and service reconstitution.   It is important to remember that in many cases the National CSIRT will not handle all of the incident handling and analysis itself. A National CSIRT may act to facilitate and coordinate analysis and response, either because of limited resources or because knowledge about the specific problem may reside elsewhere, for instance at another National CSIRT or at a technology vendor. The specific capabilities and processes needed to mange incidents will be covered in more details in the planned publication *Best Practices for National Cyber Security: Managing a National CSIRT*.

3.4.1 Enabling Goal: Define Incidents and Threats of National Interest

Resources are scarce. Defining the incidents and threats that are of interest to a National CSIRT is perhaps the most challenging task facing the National CSIRT. Determining where the National CSIRT should focus its attention is an iterative, evolving process that occurs over the course of time. It is very typical that after the initial formation of an incident management capability the National CSIRT becomes inundated with questions and requests for assistance. This places the National CSIRT in the position of having to balance the scarcity of time and resources with a desire to serve the community and build its relationships with stakeholders. Managing this tension and improving the process performance of National CSIRTs will be discussed in more detail in future volumes in this series.

During the process of building the National CSIRT capability there are several resources that will help the sponsor define the initial focus areas for the National CSIRT. These include the following:

- Information systems and incidents that affect those critical infrastructure sectors identified in the National Cyber Security Policy, if there is one. This should be the primary initial driver behind the National CSIRT focus areas. Providing guidance to the National CSIRT is one of the principle reasons for having a coordinated national policy.
- Incidents and threats that may affect systems in one or more sectors of critical infrastructure.
- Types of incidents or activity that may be of unique concern to national authorities because they may directly affect national security, result in revealing sensitive information, cause embarrassment to the nation, or because of other unique factors.
- Incidents that substantially affect a majority of computer users in the general public.
- The knowledge and experience of the National CSIRT's staff.
- Types of threats that are judged by the National CSIRT's incident analysts and the incident response community as part of greater or evolving threats.
- The knowledge and shared wisdom from other National CSIRTs

Having an awareness of the systems currently in use by the National CSIRT's key constituents can also help the National CSIRT focus its analysis of incidents. This awareness is built over time through handling incidents and interacting with the community.

3.4.2 Enabling Goal: Analyze Computer Security Incidents

All National CSIRTs must possess the capability to respond to cyber incidents and provide the community with analysis and support. Not all National CSIRTs will have identical specific capabilities to do this work. For instance, National CSIRTs will not all have the same level of external partnership with information technology experts, software development communities, and security researchers. Nor will all National CSIRTs have internal teams to perform code-level analysis of malware and software (the latter to determine vulnerabilities) and to replicate attacks and exploits. However, at a minimum National CSIRTs should analyze reports of problems for shared characteristics, to determine their importance and accurately gauge the level of threat represented by the problem. Shared characteristics may include such things as attack vector and attack targets. In some cases, these shared characteristics may involve identifying or attribution information that can be useful to the nation's security services.

3.4.3 Enabling Goal: Develop an Efficient Workflow Process

A National CSIRT will inevitably receive information from multiple sources about computer security incidents. These notifications will come via email, web form, telephone, fax, or automated process (i.e., event notification from automated information systems and sensors). Personal reports (i.e., those from individuals rather than information systems) should be expected from both known and unknown sources. Known sources include operating partners, information sharing networks, trusted members of private industry, government stakeholders, and significant domain subject matter experts (research scientists, etc). Unknown sources may include reports from citizens and other organizations where a relationship does not exist. One example is the "hotline," which is a posted phone number or instant messaging service which allows all parties to report incidents to the National CSIRT 24 hours a day and 365 days a year. These incidents will vary in their severity and importance.

In order for the National CSIRT to efficiently and fairly handle reports it should establish a clear, consistent workflow process. Typical steps would include

- Determine whether the incident will be handled by the National CSIRT.
- Collect and document incident evidence.
- Analyze and prioritize Incident Reports. Determining the importance of the incident and distributing the work within the National CSIRT is an important component of efficiently using resources.
- Analyze incidents.
- Respond to and recover from incidents.
- Close incidents.

3.4.4 Enabling Goal: Warn the Community

The National CSIRT warns the community it serves for a number of reasons. Timely notification of a threat can be the difference between protecting a system or systems from attack, and recovering from an incident. Warnings and alerts increase the ability of the affected constituents to prepare against and detect threats and vulnerabilities, reducing the potential impact of risk. Warning the community about relevant problems will foster healthy relationships, and promote practices for situational awareness. It also can provide evidence for the "value-added" benefit of a National CSIRT.

A National CSIRT uses its relationships with stakeholders and with other National CSIRTs, as well as its collected incident reports and analysis of those reports, to learn about threats and vulnerabilities and identify information that needs to be distributed to the community. A National CSIRT must design warnings to inform the community and encourage them to act to defend themselves. However the National CSIRT must balance the need to disseminate the information quickly with the sensitivity of the information and the format of the warning. Such warnings must be sent to the community in a manner that provides for its authenticity, integrity, and privacy where required. In addition, some warnings require confidentiality regarding the source of the information, particularly in cases where an intelligence source supplies threat information. Care needs to be exercised to ensure that while relevant threat information is effectively shared, it is not shared to those without a need to know. Many National CSIRTs strive to remove information that may indicate the source of threat and vulnerability data, limiting communications to the vulnerability discovered or obscuring specific threat data.

Warnings from the National CSIRT to stakeholders and the national community in general are typically more effective when transmitted through trusted, confidential communications channels that have already been established. These "channels" may take the form of specific individuals or offices in key organizations. Working through pre-established confidential communication mechanisms has proven to be a very successful strategy for building trusted relationships between the National CSIRTs and their stakeholders and constituents. As a basis of the trusted relationships, National CSIRTs and their stakeholders and major constituents agree upon the communications method, the terms of information handling, and other protections. This enabling goal is closely tied with establishing trusted communications.

3.4.5 Enabling Goal: Publicize Cyber Security Best Practices

A National CSIRT collects information about security problems through a defined incident management process, through the research it performs, and through information sharing with communities and other National CSIRTs. Through the incident response function specifically, National CSIRT's collect historical knowledge which is an excellent source of "Lessons Learned." The lessons extracted from a number of incidents form the basis for targeted skills development and general security awareness, and they often improve situational awareness and contribute to overall cyber risk management. A National CSIRT may communicate best practices it has codified through the publication of general cyber security best practice documents, guidance for incident response and prevention, training, recommended organizational procedures, and published case studies of practice adoptions. For example, a National CSIRT may produce best practices about:

- How to secure specific technologies against known attacks and cyber security threats.
- How to develop, test, and exercise emergency response plans, procedures, and protocols.
- How to coordinate with the National CSIRT on security research (e.g., vulnerability identification, root cause analysis, and threat and attack community research).

3.4.6 Additional Resources: For Establishing Situational Awareness and Managing Incidents

The following is a list of publicly available resources for establishing cyber security awareness and managing incidents:

Reference materials

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): http://www.cert.org/octave/

- CERT Resiliency Management Model (RMM): http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm
- FIRST Papers & Presentations related to Computer Security: http://www.first.org/resources/papers/index.html
- FIRST Best Practices Guides: http://www.first.org/resources/guides/index.html
- ENISA Quarterly Review: http://www.enisa.europa.eu/publications/eqr

Training resources

- CERT Assessing Information Security Risk Using the OCTAVE Approach: http://www.sei.cmu.edu/training/p10b.cfm
- CERT OCTAVE Approach Instructor Training: http://www.sei.cmu.edu/training/p42b.cfm
- CERT Computer Security Incident Handling Certification: http://www.sei.cmu.edu/certification/security/csih/
- FIRST Network Monitoring SIG meetings: http://www.first.org/meetings/nm-sig/
- Computer Security Incident Handling: http://www.first.org/conference/
- CERT Virtual Training Environment: https://www.vte.cert.org/vteweb/default.aspx
- FIRST Technical Colloquia & Symposia: http://www.first.org/events/colloquia/
- SANS courses: http://www.sans.org/security-training/courses.php

Materials on Warning the Community

- United States Department of Homeland Secuirty Stay Safe Online Website: http://www.staysafeonline.org/ncsam
- The United States' US-CERT maintains a repository of cyber security situational awareness information: http://www.uscert.gov/
- US-CERT Vulnerability Notes Database: https://www.kb.cert.org/vuls/
- National Institute of Standards and Technology: National Vulnerability Database: http://web.nvd.nist.gov/view/vuln/search
- Australia's Stay Smart Online Alert Service: https://www.ssoalertservice.net.au/
- United Kingdom's Warning, Advice, and Reporting Point's newsletters: http://www.warp.gov.uk/Index/WARPNews/indexnewsletter.htm
- International Telecommunications Union's collection of Security Alert Providers: http://www.itu.int/osg/spu/ni/security/links/alert.html

3.5 Strategic Goal: Support the National Cyber Security Strategy

A National CSIRT is a significant operational component of a national approach to executing cyber security strategy. A National CSIRT participates within a broader context for national incident management against a host of diverse threats (i.e., man-made and natural; physical and cyber). A National CSIRT can be used to help

- determine additional national strategic requirements for cyber security
- identify needed technical practices, educational improvements, skills development of cyber security practitioners, and research and development
- identify opportunities to improve cyber security laws and regulations
- distribute lessons learned from cyber security experiences affecting the national approach to cyber security itself
- improve the measurement of damages and costs associated with cyber incidents

Perhaps most importantly for the national cyber security strategy, the National CSIRT can help promote a national culture of cyber security. By bringing together diverse stakeholders, the National CSIRT can help stakeholders better understand cyber security issues and the importance of this area to their various communities.

3.5.1 Enabling Goal: Translate Experiences and Information to Improve National Cyber Incident Management and Cyber Policy Development

While organizations of all sizes will continue to perform internal cyber incident management, a National CSIRT alone has the primary responsibility of addressing national level concerns. Translating National CSIRT experiences in a way that is useful to policymakers, stakeholders, and the community of security practitioners generally enhances national cyber security. Translating experiences implies considering ways in which the National CSIRT's work and the experiences of the community may have broader implications for national laws and policies. This translation can produce lessons-learned and improve problem avoidance and risk mitigation nationally, as well as influence national regulations, guidance, initiatives and directives.

One example of such an experience may include incidents involving vulnerabilities affecting a system the national government is considering deploying across its departments, agencies, and ministries. Understanding the inherent risks may determine whether it will choose a technology or not. Another example may involve some ambiguity or inconsistency in privacy law that impedes information sharing among private stakeholders. The sources for these lessons learned include both the National CSIRT's experiences and the experiences of stakeholders.

3.5.2 Enabling Goal: Build National Cyber Security Capacity

A National CSIRT is uniquely situated to serve as a trusted, national focal point. By taking advantage of this, a National CSIRT can coordinate with all owners and operators of ICT (private and/or public) to gain a uniquely comprehensive perspective of the national cyber security landscape. This allows the National CSIRT to support the national cyber security strategy, manage incidents of national concern, and support government operations most effectively. A National CSIRT typically builds national cyber security capacity by publishing best practices and providing services, guidance, training, education, and awareness for the building of other organizational CSIRTs.

A National CSIRT is well positioned to foster a broad-based national culture of cyber security. Publications and advisory services of the National CSIRT should be designed to build collective national capability, rather than cater to specific niche needs.   It is incumbent on a National CSIRT not to act in the capacity of advocating the interests of a particular stakeholder. The National CSIRT can act as a valuable bridge between stakeholders and national policymakers. The extent to which a National CSIRT can fulfill this role may depend on legal and structural factors. However, within these constraints the National CSIRT can help policy makers understand and appreciate the views and constraints of other stakeholders and catalyze meaningful discussion of complex issues.

3.5.3 Enabling Goal: Leverage Public Private Partnerships to Enhance Awareness and Effectiveness

Protecting critical infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government and the private sector, which often owns and operates much of the infrastructure. Successful government-industry collaboration requires three important elements: (1) a clear value proposition; (2) clearly delineated roles and responsibilities; and (3) bidirectional information sharing. The success of the partnership depends on articulating the mutual benefits to government and industry partners. The benefits to governments include, among others:

- influence on the protection of national critical infrastructure that is not owned or operated by the government
- increased situational awareness through robust bidirectional information sharing

In assessing the value proposition for industry, there are clear benefits to working with government to enhance cyber security, which include:

- access to actionable information regarding critical infrastructure threats
- increased sector stability that accompanies proactive risk management
- opportunity to influence related policy and initiatives

National CSIRT operational and strategic capabilities require active participation from all its partners. Governments and industry should collaboratively adopt a risk management approach that enables government and the private sector to identify the cyber infrastructure, analyze threats, assess vulnerabilities, evaluate consequences, and identify mitigations plans. The capability of the National CSIRT to prioritize threats is also enhanced by the collaborative identification of privately owned critical infrastructure.

3.5.4 Enabling Goal: Participate In and Encourage the Development of Information Sharing Groups and Communities

The National CSIRT's participation in information sharing groups and communities is an important way to enhance situational awareness and build trust relationships. Information sharing in this context should ideally be bi-directional between the National CSIRT and its community. With regard to infrastructure operators specifically, incident and risk information should flow to the National CSIRT from industry while the National CSIRT in turn disseminates threat, vulnerability, and mitigation information. Government, the National CSIRT, and industry can enhance this information flow by collaboratively developing a formal framework for incident handling, including issues surrounding information sharing. The framework should include policies and procedures for sharing information and reporting incidents, protecting and disseminating sensitive (government and industry) proprietary information, and mechanisms for communicating and disseminating information.

There are several different types of information sharing groups. Where the National CSIRT identifies a need for a particular venue in which to share information, it should take the lead in establishing such an organization.

Industry groups are comprised of separate firms in the same industry, for instance the several electrical suppliers in a nation. These groups are often a valuable source of information about vulnerabilities and incidents in a particular industry and can be fruitful venues to catalyze discussion about cyber security. While industry groups are very beneficial, participants may sometimes be reluctant to share proprietary or sensitive information in a group of their competitors.

Communities of interest are generally groups with a narrow, technology focus. These groups are integral components of information sharing because they often have deep technical knowledge, skills, and experience to study a problem and create solutions. Participants in these groups are often individuals recognized for their technical skills, leading researchers in the fields of cyber security and computer science, and private industry representatives from key information and communications technology providers (i.e., infrastructure providers, software developers, etc).

In some countries, communities of interest already share information on security threats, vulnerabilities, and impacts. Often, these groups also provide timely alerts and warning to members to facilitate efforts to mitigate, respond to, and recover from actual incidents impacting the critical infrastructures. Examples of these groups include Information Sharing and Analysis Centers (ISACs) in the United States, and Warning, Advice, and Reporting points (WARPs) in the U.K.

Government-Industry working groups can greatly facilitate information sharing**.** Government can be informed by industry, soliciting comments from industry for cyber security policy and strategy development, and coordinating efforts with private sector organizations through information sharing mechanisms. Government should ensure that the private sector is engaged in the initial stages of the development, implementation, and maintenance of initiatives and policies. Industry can benefit from these groups by gaining the opportunity to affect policy making and learning how their sector fits in the overall national defense picture.

Finally, the National CSIRT can play an important role organizing working groups among interdependent industries. Incidents involving one infrastructure sector can have cascading effects that result in incidents in others, creating interdependencies that are not always anticipated. For example, service disruptions in one public utility may create high volumes of customer calls, disrupting telephone networks. By developing an understanding of how cyber security affects multiple systems, the National CSIRT can play an important role in helping infrastructure owners and other organizations be sensitive to these interdependencies. Sharing information across infrastructure firms can facilitate the response to incidents that cut across multiple sectors.

3.5.5 Enabling Goal: Assist the National Government in Responding to Incidents in Support of Government Operations

Where it is appropriate, based on political and organizational considerations, the National CSIRT enhances its role and effectiveness by handling incident response for government entities. Doing so helps to build trust relationships with government departments and helps the National CSIRT maintain an awareness of the systems and technology currently in use. In cases where incident response in specific departments is handled by an in-house CSIRT, for instance a CSIRT dedicated to the nation’s armed forces, the National CSIRT can provide support by disseminating threat information and information obtained through outreach with the nation's various organizational CSIRTs.

3.5.6 Additional resources: Support the National Cyber Security Strategy

The following is a list of publicly available resources for understanding how National CSIRTs support a national cyber security strategy.

Reference materials

- DHS National Infrastructure Advisory Council: Reports and Recommendations: http://www.dhs.gov/files/committees/gc_1227558980345.shtm
- US-CERT Government Collaboration Groups and Efforts to support government infrastructure: http://www.uscert.gov/federal/collaboration.html
- The National Council for Public-Private Partnerships (U.S.): http://www.ncppp.org/
- Partnership for Critical Infrastructure Security: http://www.pcis.org/
- DHS Sector-Specific Plans: http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- CSIRTs and WARPs: Improving Security Together: http://www.warp.gov.uk/Marketing/WARPCSIRT%20handout.pdf

4 Case Study: Components of the National Policy on Cyber Security in the United States

4.1 National Response Framework

The National Response Framework details how the U.S. conducts an all-hazards response to incidents – from the smallest incident to the largest catastrophe. The National Response Framework identifies the key response principles, as well as the roles and structures that organize national response. It describes how communities, states, the federal government, and private-sector partners apply these principles for a coordinated, effective national response. In addition, it describes special circumstances where the federal government exercises a larger role, including incidents where federal interests are involved and catastrophic incidents where a state would require significant support. It lays the groundwork for first responders, decision-makers and supporting entities to provide a unified national response.

4.2 National Infrastructure Protection Plan

The Secretary of the Department of Homeland Security developed the National Infrastructure Protection Plan (NIPP) with the goal of protecting the country's critical infrastructure and key resources. It provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation under a single national program. The overarching goal of the NIPP is to build a safer, more secure, and more resilient United States by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of the United States' critical infrastructure. It is also designed to strengthen national preparedness, ensure timely response and rapid recovery of critical infrastructure in the event of an attack, natural disaster, or other emergency. The NIPP specifies the key initiatives and milestones required to achieve the United States' protection mission, including a comprehensive risk management framework.

The NIPP formalizes the collaboration between government and industry through a Sector Partnership Model. This model includes Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) comprised of industry and government representatives who work together to address risk by analyzing consequences, vulnerabilities, and threats.

The NIPP relies on the sector partnership model as the primary organizational structure for coordinating the nation's Critical Infrastructure/Key Resources (CI/KR) protection mission. For each critical infrastructure and key resources sector, a Sector Coordinating Council representing the private sector and a Government Coordinating Council have been created to share data, techniques, best practices, and to support systematic risk-based planning. The DHS provides guidance, tools, and support to assist these sector-specific groups in working together to carry out their responsibilities.

The NIPP's complementary Sector-Specific Plans (SSPs) detail the approach to CI/KR protection goals, initiatives, processes, and requirements for each sector. SSPs are developed by the designated Sector Specific Agency (SSA) in coordination with their public and private sector security partners. The SSPs reflect a consensus starting point, demonstrate progress made, and provide a path forward for further protection activities. Each SSP is reviewed on an annual basis and updated regularly, as appropriate. They provide the mechanisms for

- identifying assets – including cyber assets, systems, and networks
- assessing risk – including understanding threats, assessing vulnerabilities and consequences
- implementing information-sharing and protection measures within and across CI/KR sectors

4.3 Critical Infrastructure and Key Resources

Homeland Security Presidential Directive 7 (HSPD-7) "Critical Infrastructure Identification, Prioritization, and Protection," identifies critical infrastructure sectors that the public and private sectors must work jointly to protect. While definitions may vary slightly, critical infrastructures (CI) are generally considered as the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those matters. CI is composed of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data).

The following eighteen CI/KR sectors have been identified in the U.S.:

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Drinking Water and Water Treatment Systems
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation Systems

4.4 National Strategy to Secure Cyberspace

Published in 2003, the National Strategy to Secure Cyberspace is part of the overall effort to protect the U.S. The Strategy was developed under a White House advisory group called the Critical Infrastructure Protection Board (CIPB) and in consultation with government agencies, the private sector, and civil society. Once DHS was formed, the functions of the CIPB were absorbed into DHS.

The purpose of the document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the Federal Government, state and local governments, the private sector, and the American people.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the National Strategy to Secure Cyberspace are to

- prevent cyber attacks against America's critical infrastructures
- reduce national vulnerability to cyber attacks
- minimize damage and recovery time from cyber attacks that do occur

4.5 United States Computer Emergency Readiness Team (US-CERT)

Created in 2003 by the National Cyber Security Division of the Department of Homeland Security, US-CERT serves as a focal point for national cyber security coordination. US-CERT fulfils strategic goals common to National CSIRTs. Specifically it;

- manages incidents of national concern
- supports national cyber security strategy
- supports government operations
- serves as a trusted communications partner

US-CERT groups its mission responsibilities into three main categories

- Information Sharing and Coordination: Informing national, state, and local government agencies, private sector partners, infrastructure owners and operators, and the public about current and potential cyber threats and vulnerabilities.
- Alert, Warning, and Analysis: Compiling and analyzing information about cyber incidents.
- Response and Assistance: Providing timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents.

The operational components of the US-CERT responsibilities can be detailed into five categories:

- Threat: Prioritization and mitigation
- Vulnerability: Prioritization, reducing attack surface and ensuring proper configuration
- Attack Detection: Early warning
- Mitigation: Preventing the attack
- Reflection: Changing policy, procedures and technology to prevent reoccurrence

US-CERT produces a range of free, timely, and actionable information to improve the cyber security posture for all citizens. The National Cyber Alert System is an array of targeted communications operated by US-CERT to advise both technical and non-technical stakeholders. Technical Security Alerts and Security Bulletins provide detailed explanations of system vulnerabilities and recommended remediation. For instance, in March of 2009 US-CERT analyzed the Conficker/downadup computer worm and issued a diagnostic tool to help key communities determine if their systems were detected. Information and guidance was also provided to home users. US-CERT issues Security Alerts and Security Tips to convey vulnerability information to non-technical audiences. Federal agencies receive Federal Information Notices and periodic Trend Analysis Reports, and partners in private industry are provided Critical Infrastructure Information Notices.

5 Conclusion

As nations recognize that their critical infrastructure has integrated sophisticated technologies to provide greater efficiencies and reliability, they acknowledge the need to effectively manage risks arising from those technologies. Instituting a national computer security incident management capability can be a very valuable step towards helping nations manage risk and secure their systems. This capability is referred to in this document as the National CSIRT. The challenge faced by National CSIRT sponsors is the lack of information that provides guidance for and describes how a National CSIRT fits in the context of a national cyber security policy, the strategic goals for a National CSIRT, and the goals and principles that support the capability. This document provides insight that interested stakeholders and governments can use to begin to develop a National CSIRT capability and determine its role within a strategy of national cyber security. Strategic goals of the National CSIRT are provided, along with enabling goals and considerations. Where additional resources are accessible, such as publicly available training and reference materials, they have been included to allow the reader to obtain a deeper understanding of the issues surrounding these cyber security issues and challenges of National CSIRTs.

This handbook is designed to be introductory curricula for cyber security capacity development within nations. The intended audience includes potential sponsors of National CSIRTs, government policymakers, and individuals responsible for information and communications technologies wanting to learn more about the value proposition of National CSIRTs and incident management capability generally. It is not intended to be a guide on the daily operations of a National CSIRT, but as informative materials on how a computer security incident management capability may support a national cyber security strategy.

The simple truth is that there is a common need to resist, reduce, and fight cyber threats and respond to attacks. National CSIRTs and organizations like them provide a domestically-focused, internationally-amplified operational response to those cyber incidents that can destabilize critical infrastructure.

References

URLs are valid as of the publication date of this document.

[Brunner 2009]

Brunner, Elgin M. & Suter, Manuel. *International CIIP Handbook 2008/2009.* Zurich, Switzerland*:* Swiss Federal Institute of Technology Zurich. 2009. *http://www.css.ethz.ch/publications/CIIP_HB_08*.

[DHS 2003]

Department of Homeland Security. *The National Strategy to Secure Cyberspace.* Washington, D.C. 2003. *http://www.dhs.gov/files/publications/publication_0016.shtm*.

[DHS 2008]

Department of Homeland Security. *National Response Framework.*Washington, D.C. 2008. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[DHS 2009]

Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*. Washington, D.C. 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[Killcrece 2004]

Killcrece, Georgia. *Steps for Creating National CSIRTs.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. 2004. http://www.cert.org/csirts/national/.

[West-Brown 2003]

West-Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs).* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. 2003. http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE June 2010	3. REPORT TYPE AND DATES COVERED Final

4. TITLE AND SUBTITLE

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

5. FUNDING NUMBERS

FA8721-05-C-0003

6. AUTHOR(S)

John Haller, Bradford J. Willke, Samuel A. Merrell, Matthew J. Butkovic

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

CMU/SEI-2010-SR-009

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified/Unlimited, DTIC, NTIS

12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

As nations recognize that their critical infrastructures have integrated sophisticated information and communications technologies (ICT) to provide greater efficiency and reliability, they quickly acknowledge the need to effectively manage risk arising from the use of these technologies. Establishing a national computer security incident management capability can be an important step in managing that risk. In this document, this capability is referred to as a National Computer Security Incident Response Team (National CSIRT), although the specific organizational form may vary among nations. The challenge that nations face when working to strengthen incident management is the lack of information that provides guidance for establishing a capacity appropriate to the nation, understanding how it supports national cyber security, and managing the national incident management capability. This document -first in the Best Practices for National Cyber Security Series - provides insight that interested organizations and governments can use to begin to develop a national incident management capability. The document explains the need for national incident management and provides strategic goals, enabling goals, and additional resources pertaining to the establishment of National CSIRTs and organizations like them.

14. SUBJECT TERMS

Cyber security, incident response, national security

15. NUMBER OF PAGES

40

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL