Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?
Check out the list of upcoming events offering "Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec
Critical Infrastructure Protection: Establishing an Information Sharing and Analysis Center (ISAC) Can Be Like Developing an Organizational Security Policy
Frances Wentworth
September 26, 2000

Purpose
This paper describes two existing Information Sharing and Analysis Centers (ISACs) that support national goals of Critical Infrastructure Protection, while drawing some parallels between establishing ISACs and developing organizational security policies.

Introduction
Information security is a goal of all businesses and governmental organizations today, and developing an organizational security policy is a basic step towards achieving organizational security. Bearing in mind the old expressions, "The whole is greater than the sum of its part," or "A chain is only as strong as its weakest link," one can recognize that it is a rare organization today that can stand alone and not be impacted by what happens to its business partners, customers, suppliers, or colleagues in the industry. And, clearly, the Internet can be a threat as well as a necessity. It is not enough to guarantee the security of single organizations. What could organizations do to enhance the security of the national environment within which they operate? And what about the impact that failures in key industries could have on other industries and even the national economic structure?

Critical Infrastructure Protection

Enter the concept of Critical Infrastructure Protection. In October 1997, after 15 months of study, the President's Commission on Critical Infrastructure Protection (PCCIP) published a report highlighting the widespread and growing capability to exploit infrastructures, especially through information networks. The PCCIP report defined critical national infrastructures as energy, banking and finance, transportation, vital human services, and telecommunications. A key point in the report was that the nation's critical infrastructures are mainly privately owned and operated, therefore, their protection should be a shared responsibility of the public and private sectors.

In May 1998, the White House issued Presidential Decision Directive (PDD) 63 in order to build on the recommendations of the PCCIP report and develop a framework for critical infrastructure protection. One of its goals is to "[seek] the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships...". The supporting White Paper on Critical Infrastructure Protection further explained key elements of PDD 63. It expanded the previous definition of critical infrastructure to "those physical and cyber-based systems essential to the minimum operations of the economy and government", [including, but] "not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."

PDD-63 established a structure within the US government to include a National Coordinator, National Infrastructure Protection Agency (NIPC), Information Sharing and Analysis Centers (ISACs), National Assurance Council (NIAC), and Critical Infrastructure Assurance Office (CIAO). The White Paper also designated lead agencies to be "sector liaisons" for the various critical infrastructure areas. For example, the Department of Commerce is the sector liaison for the Information and Communications sector, and the Department of the Treasury is sector liaison for the Banking and Finance Sector.

What is an "ISAC"?

An ISAC is the method to facilitate information sharing among members of a particular industry sector, and between that sector and the government (the NIPC), and, by extrapolation, between that sector and other sectors. According to the White Paper, the "actual design and functions [of an ISAC] and its relation with the NIPC will be determined by the private sector,"... " with the intent that an ISAC would "serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC". Although the language in PDD-63 refers to plural Information Sharing and Analysis Centers (ISACs), the description in the White Paper refers to "a(n)" ISAC, as a singular noun. In actual practice, and apparently well in line with the intent of PDD-63, multiple ISACs are being established within the various sectors.

Why compare establishment of an ISAC to development of a Security Policy?

How does the process of establishing ISACs resemble security policy development?
Clearly, the purpose of both is to enhance security, one for a single organization, the other for an entire industry sector and the nation at large. Organizational security policies and ISACs both aim to protect information and physical assets. In a sense, an ISAC can function as a super-security organization, or function, within its industry sector, because it is the mechanism to link individual organizations and share information to enhance the security of all members. In addition, the decision processes used to define and establish an ISAC are similar to the decision processes needed to develop and implement an organizational security policy.

Two Existing Models of an ISAC

Just as one organization’s security policy may not fit the requirements of another organization, there can also be multiple successful incarnations of an ISAC. There is no one right answer for either a security policy or an ISAC structure, but each will have common elements. This paper uses the first two actual ISACs as models for illustration—one from the banking and finance sector, and one from the telecommunications area, which is a subset of the Information and Communications sector.

Model 1: Financial Services ISAC (FS/ISAC)

The Financial Services ISAC (FS/ISAC) declared itself operational on October 1, 1999. It was established as a limited liability corporation (LLC), with membership open to FDIC insured banks, NASD licensed investment firms, designated financial services exchanges and finance sector utilities, specialized US or State licensed banking companies, and US or State licensed insurance companies. The actual member list is not releasable to anyone, due to the guiding principle that "anonymity of members is key to obtaining industry-wide cooperation." Note that there is no category for governmental members, which makes this a private sector-only ISAC.

The FS/ISAC "is a secure database that provides for authenticated and anonymous sharing of information associated with threats, incidents, and vulnerabilities of industry assets and available resolutions or solutions. FS/ISAC will be Internet based, allowing authorized participants to securely share information with other authorized members of the financial services industry. A team of analysts and security professionals will assess each submittal, qualify and quantify the seriousness of the vulnerability or attack, and identify patterns that might represent a coordinated assault." Note that the mission of the FS/ISAC is to share, analyze, and disseminate information related to cyber threats, as opposed to all threats.

Model 2: National Coordinating Center for Telecommunications ISAC (NCC-ISAC)

The first public acknowledgement of the existence of the NCC-ISAC occurred during a White House press briefing on January 7, 2000. The purpose of the briefing was to describe the progress made in protecting critical infrastructures since the signing of PDD-63, and to announce the release of Version One of the National Plan for Information Systems Protection. It described the Plan’s two broad goals as "establishment of the U.S. government as a model of information security, and the development of a public-private partnership to defend our national infrastructures." One of the key initiatives covered in the briefing was Information Sharing and Analysis Centers: "Two of the proposed six private sector computer security centers have been established (banking and finance and telecommunications)." These remarks refer to the FS/ISAC and NCC-ISAC, respectively.

The National Coordinating Center for Telecommunications (NCC) was established in 1984 as a joint industry-government organization to "assist in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness (NS/EP) telecommunications services and facilities under crisis or emergency conditions." As such, it was a pre-existing organization that added the ISAC function to its mission following the signing of PDD-63. The mission of the NCC-ISAC is to gather, analyze, and share, among participants, telecommunications information on vulnerabilities, threats, intrusions, and anomalies.

Industry membership in the NCC is open to "all U.S. telecommunications industry entities that provide domestic or international communications services; local or long-haul communications services; voice or data (including software) communications services; or telecommunications equipment supply services". During the initial phase of the NCC-ISAC, participants consist of the existing and any pending members of the NCC. Subsequent phases of the NCC-ISAC will promote expansion of participation to include [industry] "providers and operators of wireless services, Internet services, data transmission services, cable services, and providers of database and gateway services to infrastructure operators."

Due to the joint industry-government nature of the NCC-ISAC, there are some legal impediments to information sharing that do not pose a problem for the private-sector only structure of the FS/ISAC. The main impediment is the requirements of the Freedom of Information Act (FOIA), which provides the public access to records maintained by
the government, and which, therefore, could potentially threaten release of private sector data shared with the government participants in the NCC-ISAC.

Making Choices

Although both the FS/ISAC and the NCC-ISAC were created in response to PDD-63, the above descriptions show some fundamental differences between the structure and policy of the two.

FS/ISAC: Private sector members only
- Actual member list not releasable
- Emphasis on complete anonymity of inputs from members
- Threat and mission focus on cyber threats only

NCC-ISAC: Private and public sector partnership
- Members identified
- Concern with legal impediments to information sharing among participants
- Threat and mission focus on all threats, including cyber

Some of the thought processes used to make these choices may be viewed as a macrocosm of the process used to establish an overarching organizational security policy. Decisions on threat, mission focus, membership eligibility, information sharing rules, etc. are determined by any organization and the choices set the tone for any subsequent policies and procedures developed.

Common elements among the two example ISACs are those functions intended by PDD-63, but (also intended by PDD-63) with a flavor and format determined by the particular industry establishing the ISAC. The common threat element is the national cyber threat (which was the main purpose of PDD-63), however, the NCC-ISAC includes non-cyber anomalies as well.

Different industry requirements, mission, potential impacts of compromise of data, specific threats, and the "ISAC organizational policy" will drive additional policies or interpretations of threats. An internal threat for any ISAC with private sector membership, is the risk to proprietary or sensitive information from fellow ISAC members who are competitors. The FS/ISAC addresses this through strong emphasis on anonymity; the more open sharing within the NCC-ISAC (i.e., no guarantee of anonymity), in theory, offers more of an "insider threat," whether or not that threat may be an actual concern among the participants. Additionally, the participation of government agencies within the NCC-ISAC adds a threat to information protection through the risk of FOIA requests.

Who should have access to what information is a critical consideration in developing any security policy. It is equally, if not more, critical in formation of an ISAC, since basic policy for access to information is prerequisite to actually creating the ISAC. For the FS/ISAC, the first "access" decision was to become a private-sector only ISAC; for the NCC-ISAC, the decision was to retain its private-public partnership. The next access policy decision was determining who within the given industry sector could be members, since all non-members would be excluded from access to the information from the ISAC (unless, as intended by PDD-63, the ISAC shares some information with the NIPC or other entities who are not members). The FS/ISAC made an additional policy decision when it adopted the concept of anonymity among members.

How the policy for access is implemented and controlled is also an important consideration in developing security policy and procedures. The implementation of ISAC sharing agreements and procedures can be seen to derive from the previous basic access policy decisions. Both the FS/ISAC and the NCC-ISAC address the issues of safeguards when sharing information among their respective members. The FS/ISAC emphasizes the total anonymity of the members who provide data and offers to prove the robustness of its technical procedures to any prospective member. The NCC-ISAC follows a more open sharing policy among its participants, however, due to the participation of government agencies, is burdened with the risk of FOIA requests for data, as previously mentioned.

Conclusion

Recognizing elements of security policy development processes can help in understanding choices made in development of Information Sharing and Analysis Centers for critical infrastructure protection. There are common
elements among ISACs, but there is no one right answer in establishing an ISAC. Early organizational decisions will produce the overarching policy and guiding principles that drive ISAC operation.

Endnotes


2. Ibid., Executive Summary


4. Ibid.


6. Ibid., Section I

7. Ibid., Annex A, "Structure and Organization"

8. Ibid., pp. 10-11


11. Ibid.

12. Financial Services Information Sharing and Analysis Center press release


15. White House Press Briefing


20. NSTAC Report, pp. 4-5
21. Ibid., p. 5
22. Ibid., Section 2.1.4.3, "Legal Impediments", p. 9
23. National Coordinating Center for Telecommunications Fact Sheet
25. Financial Services Information Sharing and Analysis Center, Frequently Asked Questions

References


Financial Services Information Sharing and Analysis Center, Overview, URL: http://www.fsisac.com/fsisac_overview.htm (19 Sept 2000)


Financial Services Information Sharing and Analysis Center, Membership Agreement, URL: http://www.fsisac.com/MembershipAgreement.pdf

Financial Services Information Sharing and Analysis Center, Member Enrollment Process, URL: http://www.fsisac.com/fsisac_enroll.htm (19 Sept 2000)


Financial Services Information Sharing and Analysis Center, press release, "Global Integrity Announces That The Financial Services Information Sharing And Analysis Center Will Be Fully Operational On October 1; Global Integrity Serves As FS/ISAC Administrator", URL: http://www.fsisac.com/fsisac_pressrelease.htm


Kramer, Carol Stephen Northcutt, Fred Kerby, SANS GIAC, GIAC Basic Security Policy, Version 1.34, July 2000


President’s Commission on Critical Infrastructure Protection (PCCIP) Report, Critical Foundations: Protecting America’s Infrastructures, October 1997,

The White House, *Defending America’s Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, January 2000,

White House Press Briefing, "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century," January 7, 2000,

## Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Munich March 2020</td>
<td>Munich, Germany</td>
<td>Mar 02, 2020 - Mar 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Spring 2020</td>
<td>Reston, VA</td>
<td>Mar 02, 2020 - Mar 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2020</td>
<td>Tokyo, Japan</td>
<td>Mar 02, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS St. Louis 2020</td>
<td>St. Louis, MO</td>
<td>Mar 08, 2020 - Mar 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Dallas 2020 - SEC401: Security Essentials Bootcamp Style</td>
<td>Dallas, TX</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Canadians Academy SEC401</td>
<td>Brampton, ON</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst New Career Academy SEC401</td>
<td>Brampton, ON</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS Prague March 2020</td>
<td>Prague, Czech Republic</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2020</td>
<td>Dallas, TX</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>CS-Cybersecure Catalyst Women's Academy SEC401</td>
<td>Brampton, ON</td>
<td>Mar 09, 2020 - Mar 14, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS San Francisco Spring 2020</td>
<td>San Francisco, CA</td>
<td>Mar 16, 2020 - Mar 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Norfolk 2020</td>
<td>Norfolk, VA</td>
<td>Mar 16, 2020 - Mar 21, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC401</td>
<td>Charleston, SC</td>
<td>Mar 17, 2020 - May 19, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>Mentor Session - SEC401</td>
<td>Reston, VA</td>
<td>Apr 01, 2020 - Jun 10, 2020</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2020</td>
<td>Riyadh, Kingdom Of Saudi Arabia</td>
<td>Apr 04, 2020 - Apr 16, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2020 - SEC401: Security Essentials Bootcamp Style</td>
<td>Orlando, FL</td>
<td>Apr 05, 2020 - Apr 10, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Minneapolis 2020</td>
<td>Minneapolis, MN</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bethesda 2020</td>
<td>Bethesda, MD</td>
<td>Apr 14, 2020 - Apr 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Spring 2020</td>
<td>Boston, MA</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS San Diego SEC401</td>
<td>San Diego, CA</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS London April 2020</td>
<td>London, United Kingdom</td>
<td>Apr 20, 2020 - Apr 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2020</td>
<td>Austin, TX</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2020</td>
<td>Baltimore, MD</td>
<td>Apr 27, 2020 - May 02, 2020</td>
<td>Live Event</td>
</tr>
</tbody>
</table>