Global Information Assurance Certification Paper

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 Center**s** (ISAC**s**), 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/IAC: 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 polices 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

1. President's Commission on Critical Infrastructure Protection (PCCIP) Report, *Critical Foundations: Protecting America's Infrastructures*, October 1997,
URL: http://www.ciao.gov/CIAO_Document_Library/PCCIP_Report.pdf (20 Sept 2000)

2. Ibid., Executive Summary

3. Presidential Decision Directive 63, Fact Sheet, *Protecting America's Critical Infrastructures: PDD 63*, May 22, 1998,
URL: http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop
.gov.us/1998/5/26/1.text.1 (20 Sept 2000)

4. Ibid.

5. The White House, White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998,
URL: http://www.ciao.gov/CIAO_Document_Library/paper598.html (20 Sept 2000)

6. Ibid., Section I

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

8. Ibid., pp. 10-11

9. 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 (19 Sept 2000)

10. Financial Services Information Sharing and Analysis Center, *Frequently Asked Questions*, URL:
http://www.fsisac.com/fsisac_faq.htm (19 Sept 2000)

11. Ibid.

12. Financial Services Information Sharing and Analysis Center press release

13. White House Press Briefing, "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century", January 7, 2000,
URL: http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop
.gov.us/2000/1/7/7.text.1 (21 Sept 2000)

14. The White House, *Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, January 2000,
URL: http://www.ciao.gov/National_Plan/national_plan%20_final.pdf (20 Sept 2000)

15. White House Press Briefing

16. National Communication Systems Fact Sheets, *National Coordinating Center for Telecommunications Fact Sheet*,
URL: http://www.ncs.gov/Image-Files/NCS_Fact.pdf (21 Sept 2000)

17. The President's National Security Telecommunications Advisory Committee (NSTAC) *Information Sharing/Critical Infrastructure Protection Task Force Report*, Section 2.1.2.1, "National Coordinating Center for Telecommunications," May 2000,
URL: http://www.ncs.gov/nstac/NSTACXXIII/Reports/ISCIP-Final.pdf (21 Sept 2000)

18. National Communications System Fact Sheets, *Information Sharing and Analysis Center Fact Sheet*, URL:
http://www.ncs.gov/Image-Files/ISAC_Fact.pdf (21 Sept 2000)

19. National Communications System, *NCC Operating Charter*, Organizational Structure, p. 5,
URL: http://www.ncs.gov/ncc/Op_Chart/OpChart2.HTM (21 Sept 2000)

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

24. White Paper on PDD-3, pp. 10-11

25. Financial Services Information Sharing and Analysis Center, *Frequently Asked Questions*

References

Financial Services Information Sharing and Analysis Center, *About FS/ISAC*, "Join the Financial Services Information Sharing and Analysis Center and benefit from unprecedented industry-wide cooperation," URL: http://www.fsisac.com/isac.pdf (19 Sept 2000)

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, *Frequently Asked Questions*, URL: http://www.fsisac.com/fsisac_faq.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, *Member Operating Rules*, URL: http://www.fsisac.com/OperatingRules.pdf (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

Financial Services Information Sharing and Analysis Center, *Value Propositions*, URL: http://www.fsisac.com/fsisac_value.htm (19 Sept 2000)

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

President's National Security Telecommunications Advisory Committee (NSTAC) *Information Sharing/Critical Infrastructure Protection Task Force Report*, May 2000, URL: http://www.ncs.gov/nstac/NSTACXXIII/Reports/ISCIP-Final.pdf (21 Sept 2000)

National Communications System, *Government and Industry Together*, URL: http://www.ncs.gov/ncc/Gov&Ind/Gov&Ind3.htm (20 Sept 2000)

National Communications System Fact Sheets, *Information Sharing and Analysis Center Fact Sheet*, URL: http://www.ncs.gov/Image-Files/ISAC_Fact.pdf (21 Sept 2000)

National Communications System Fact Sheets, *National Coordinating Center for Telecommunications Fact Sheet*, URL: http://www.ncs.gov/Image-Files/NCS_Fact.pdf (21 Sept 2000)

National Communications System, *NCC Operating Charter,* URL: http://www.ncs.gov/ncc/Op_Chart/OpChart2.HTM (21 Sept 2000)

National Communications System, *What is the NCC?,* URL: http://www.ncs.gov/ncc/What_Is/What3.htm (20 Sept 2000)

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

URL: http://www.ciao.gov/CIAO_Document_Library/PCCIP_Report.pdf (20 Sept 2000

Presidential Decision Directive 63, Fact Sheet, *Protecting America's Critical Infrastructures: PDD 63*, May 22, 1998, URL: http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/26/1.text.1 (20 Sept 2000)

The White House, *Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, An Invitation to a Dialogue*, January 2000, URL: http://www.ciao.gov/National_Plan/national_plan%20_final.pdf (20 Sept 2000)

White House Press Briefing, "President Clinton and Vice President Gore: Promoting Cyber Security for the 21st Century," January 7, 2000, URL: http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/1/7/7.text.1 (21 Sept 2000)

The White House, White Paper, *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998, URL: http://www.ciao.gov/CIAO_Document_Library/paper598.html (20 Sept 2000)

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event