

[WP-017]

Whitepaper: Do Information Sharing & Analysis Centers [ISAC] Work?

Risks or Issues Surrounding the Development and Maintenance of CIP ISACs

Version 050131

January 2005

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my “sounding board” on this project.)

Copyright © 2005 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for discussing a possible, and/or proposed critical infrastructure protection (CIP) security issues, and is not dependent upon any specified infrastructure, architectural condition or its issue(s). Source information is through observation from previous circumstances, related online documentation, and discussions with colleagues within the security field.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

Introduction

Since 9/11, the United States federal government has created several initiatives for enhancing dependability and infrastructure security by stimulating cross-sectored action through several directives. These directives are part of a (very) large-scaled effort by the federal government to determine risk (both inherited and assumed), assess and provide recommendations by providing monitoring, detection and early warning systems against threats, and methods of information sharing within each sector.

The model outlined for Information Sharing and Analysis Centers (or “ISAC”) are communal properties specific to each sector; that is, energy has an ISAC, food production has an ISAC, telecommunications has an ISAC, and so on and so forth. The initiatives for ISACs predates 9/11 in that both public and private interests need to be communicated, shared and understood for better utilization of those sectors. As such, all sectors make up what many refer to as “critical infrastructure”. Interestingly enough, if you ask 5 different people from 5 different sectors (still today) on the definition or term of “critical infrastructure”, you will receive 5 different answers. Fact is, the definition of “critical infrastructure” is defined in terms or perception insofar as to the area of specificity that it pertains to, is the level at which it is defined (to whomever or whatever company is defining it) as “critical” to them.



For sake of better understanding, ISACs work for each critical infrastructure sector, which includes both private and public sectors. The public sectors would be emergency management services, law enforcement, public health and welfare, fire and safety, emergency preparedness, etc. The private sectors comprise of their individual respective industries which are vital to the continued operation of the United States (as a whole). Without these industries, the United States would cease to exist – plain and simple.

How it all works

Through collaborative efforts performed through the Department of Homeland Security, public and private sector cooperation on the dependability of infrastructures, the information that it contains (which includes the development of monitoring, detection and development of early warning systems), and to improve upon cooperative efforts among various emergency response teams (of their respected sectors) is becoming clearly necessary. These recommendations for action on warning and information sharing at all levels (federal, state and local governments) reflect the intensive activities within all sectors and at a national level to improve early warning systems and methods of information sharing and collaboration.

One effort established was the United States Computer Emergency Response Team (US-CERT) group, which was spurred by an already existing suite of CERTs from varied hardware and software manufacturers (Cisco, Sun, IBM , HP, etc.), has caused these initiatives to have been comprehensively summarized into several sources. First, the DHS workshops and early warning systems at federal, state and county levels have covered EMS-related responses for just about any widespread attack that would affect government at any level. Second, the definition of a national council or committee would oversee the private sector's efforts in establishing a nationwide protocol specific to each industry for sharing, collaborating and responding to early warning detection and monitoring systems of their respective infrastructures.

The federal government has established several ISAC communities, while the private sectors have established privatized, commercial, non-profit communities of their own. Both sides continue to develop warning and information sharing systems that involve varied elements of both major sectors (public and private), and the varied embodiments and regulatory agencies and departments, etc. Though these efforts offer significant variety in the models adopted (or if they already exist, adapted) by the varied sectors, and surprisingly, there are several differences in the extent to which these systems are operated, more specifically as to the breadth of their coverage. The overall trend or eventual goal is moving towards a more integrated mechanism which openly and collaboratively includes all sectors involved by providing a more timely warning and/or information sharing system to governments, large corporations, corporate sponsors, educational institutions, and its citizens.



The dependability of implementing an ISAC-based enterprise-wide support initiative must be at a federal level, trickling downward to state and county levels insofar as to establishing a more structured and efficient protocol that lacks any possibility of error in its distinction. That is, the method by which the levels of information being shared must not deviate from the original message from the top all the way to the bottom. To this extent, the context for establishing this method of communications has been tasked to assist in the development of protocols for all actions taken by these early warning and information sharing systems (and their environments) by building upon community collaboration and trust, and clearly providing definitive goals and objectives.

Without it, the communications structure is lost, similarly to the extent that the “Voicemail Game” (a group of several individuals sits within a circle and the initial individual is given a message, directed to speak the exact message onto the next person within the chain, and so on and so forth, until the initial message is received by the initiator, often times lost in translation, either slightly or entirely, in its meaning) loses its communication.

Implement an ICS solution?

In order for any level of information sharing and collaborative efforts to be effective, participants must agree that any warning and/or information sharing system capability must ensure that an appropriate level of security be applied to ensure not only timely use of the information shared, but implements a preventative measures from outside viewing from “contaminating” the information to misinterpretation. Secondly, the appropriate levels of security information and advice provided to its users must make assumptions that its target audience has an existing level of trust and understanding; that is, the existing networks tied together that would comprise of the ISAC capability should be built upon existing trusted networks and expertise. The participants would then need to agree on the need to create a small location to facilitate these networking activities to coordinate a group of resident experts, engineers, government officials, etc., to define how the information is to be disseminated through communications channels, and to cater to the needs of their audiences who are participating with/through the early warning and/or information sharing systems.

Representatives from each ISAC must agree upon several issues and tasks for defining an early warning and/or information sharing and collaborative group such that:

- (1) Define initiatives in the area of infrastructure monitoring, detection and early warning, and define methods of information sharing and collaboration beyond the already defined and established CERT or ISAC communication channel mechanism.
- (2) Define a structured protocol for appropriate training and notification measures that work with technical and management standards, as well as any corresponding government directives.
- (3) Define and develop multidisciplinary research methods and approaches that examine all aspects of security, esp. related to several human factors dealing with psychology, sociological methods of communication and human interaction.



There is, however, a small snag in how this may be interpreted insofar as to its implementation. Concerns surrounding legal challenges, issues of protection of the data, privacy and competition between agencies and competing companies (private sectors), liabilities, intellectual property, criminal and regulatory laws insofar as to the method by which the information is to be disseminated, has all been discussed. But to what avail?

Communication channel challenges

In the relationships between commercial marketing interests and/or funding issues (mostly applied towards the private sector ISACs), representatives might emphasize more specifically upon how the communications channels as well as any financial (more importantly, revenue) streams are defined. Architectural and technical issues should be devoted to assessing and collecting data within the collection process, its processing and distribution, and the strategies as to how to go about collecting categorically all of the necessary information. This is no small task, and in fact, it may very well be continuing. Other issues might include the methods of processing, and its distribution, which might be related to discussions about technical complexities, related in how to provide/deliver data and information efficiently and effectively, and within a timely manner.

Discussions between the interested parties should define the more significant issues related to the provisional capabilities at the federal levels (both public and private sectors alike), and at the same time, continue with research and benchmarking exercises, combined with the experiences mentioned earlier, during any workshops, presentations, or seminars give, which emphasize the requirements for the varied capabilities for each area. Those capabilities would be clearly split based upon the following criteria:

- (1) Government and regulatory bodies, agencies and departments that need to be informed about vulnerabilities, interdependencies, threats, incidents, such that these groups may define strategic and tactical level policies and operating procedures for all levels of threat responses.
- (2) Industry-specific interest groups need to define methods and view of attack information sharing and collaboration databases, and should agree upon necessary data fields for defining appropriate risks associated to risk management and corporate governances.
- (3) Civil-related activities need to be defined and outlined in a manner that collects processes and disseminates data about infrastructure-related vulnerabilities, threats and risks inherent to that particular infrastructure.



However, before discussing any possible communications channel structure, any operational processes or mechanisms, it is vital that the definition of all roles and functions associated with the monitoring, detection and dissemination through either an early warning and/or information sharing and collaboration system provide the following overall objectives:

- (1) Define and establish a centralized communications channel, or contact-point, such that representatives of their specific sectors can reliably relay data and information in an efficient, effective, and timely manner.
- (2) Define and establish a provisional entity (or if it becomes necessary, entities) that defines the levels of warnings issued and how this information is to be disseminated and distributed to the community about immediate, medium or long-term risks or threats associated to their specific sectors.
- (3) Define and establish educational mechanisms that include best practices, communication channel protocols, and procedural and standards development that will foster general information security, and (ultimately) its understanding.

Since there is a community being developed, this community must have a level of understanding and comprehension that is specifically tailored to their levels of expertise. Thus, there are several audiences which would be addressed to assist in the dissemination of any threat, risk or attack. Those audiences are as follows:

- (1) Corporate and government policymakers who need reliable updates about threats, risks and potential attacks that will assess potential government and/or corporate implications.
- (2) Senior or executive management who require attack information and threat analysis that is summarized such to structure appropriate security and operational controls and corporate governance.
- (3) Emergency management who need threat data and trend analysis to plan appropriate operational and management response for enterprise-wide attacks, threats or risks of attacks that may lead to operational, market and reputation disruptions and/or regulatory and compliance failures.
- (4) General staff and personnel who may be associated with the industry or sector outlined, who need complete information and data about recent, current predicted trends from attacks to develop protection, recognition and reactionary responses.
- (5) General public who needs to be informed of any such threats, but not necessarily at a level that is overly detailed, and is less-technically specific information to operate safely, while at the same time, acquire the necessary skills to implement security management or operational procedures.



Other challenges facing ISACs

Notwithstanding whatever mechanism or funding model was chosen, any ISAC will face legal challenges that might impact its operations and abilities to disseminate and distribute threat analysis information in a timely manner.

The first level challenge addresses any administrative concerns; basically, who is going to maintain and administer the ISAC. The applicable framework may depend upon how it is incorporated and who or what is involved. For example, this entity may be considered a partnership or consortium of several interested agencies, departments and/or corporate bodies. It is viable to conceive that establishing a limited liability corporation may be worthwhile; however, if for a for-profit business model is selected, it may be conceivable to foresee a public company with some share of capital subdivided among different shareholders of it or with/through other corporate partners involved. It is also possible to consider a non-profit business model, such as an institution or consortium with a mandate to foster online trust and confidence through:

- (1) The efficient, effective and timely manner of information dissemination and its distribution about any threats, risks or potential attacks, and;
- (2) The preparation of short, medium and long-term reporting mechanisms and advisories about current and future speculations of current or foreseen challenges, threats, threat scenarios against the specific infrastructure.

Going back to the specific administrative challenges, the competition of anti-trust between corporate entities concerns may need to be addressed in case of any direct involvement between private sector entities. This may be due to the fact that these corporations rely upon “company secrets” and are viewed and treated as assets of the participating corporation; thus the dilemma of whether or not to share, disseminate and distribute information to competing corporations within the same (or even similar) industry. Assuming that the primary function of the consortium is to foster monitoring, detection and early warning, information sharing and collaboration, it is possible to speculate that it should not face anti-competitive restrictions from the consortium or institution. One method of exchanging information might be through simple exchanges of information (statistics, market research conducted from research groups or comparative studies). More importantly, it should not involve any restrictions upon any such actions or undertakings (and its recommendations) that could potentially induce other parties to behave in an identical manner.



How the data would be shared

Our federal government might want to undertake research and development projects based upon any data collected; however, the consortium might allow competing private sector corporations to cooperate, providing that the following conditions are met:

- (1) Joint research and development of products, services or processes with the notion of joint exploitation as the net result; that is, if everyone participates in a joint effort research program, everyone benefits from its outcome.
- (2) Joint exploitation of the results from the research and development that was carried out jointly pursuant to a prior, non-disclosure agreement between all interested and participating parties.
- (3) Joint research and development of products, services or processes that exclude any joint exploitation from joint research performed, and its results.

The fulfillment of these requirements, nonetheless, is not always possible, and not all corporations are willing to cooperate at this level of capacity. This highly corporate competitiveness leads to intellectual property feeding frenzies.

Legal issues and challenges

Until now, the assumption has been the establishment of a private entity in which companies, public agencies, departments and institutions would have access upon payment in some form of remediation or compensation. However, it is also possible to consider the establishment of a federal-level agency that might not be part of the outlined framework. Rather, this institution might be funded entirely by the participating groups, corporations, or public sector entities. Notwithstanding the inevitability of political concerns about staffing and location concerns, the issue would be to ensure proper and consistent access methods that are impervious to electronic attack by public and private sector organizations.

This is particularly relevant esp. if the threat, risk or potential attack data may be related to criminal offenses. Recent developments that would undermine any private or public sector efforts might either assist or hamper activities of this organization, and its abilities to disseminate and distribute information. Discussions might fail when resolved to the extent of law enforcement activities and involvement with the established organization. In general, though the entire reason for such activities is to promulgate information in a collaborative effort to stop and/or prevent such attacks, there may be circumstances in which law enforcement activities will hamper and conflict with the net result activities of the organization's primary charter. In other words, such an attack or action may mitigate the need for a lockdown as it would now be part of an investigation as evidence, thus hampering efforts to other interested parties within the ISAC who may or may not be directly involved with the investigation that may want or need said information for preventative measures in a timely fashion.



Another consideration not originally idealized was how the organization may be viewed as a liability in relation to the information it provides, disseminates and distributes. The information may or may not be correct or incorrect, or may even be delayed, such that further actions based upon the provided information might lead to additional vulnerabilities when implemented. That is, the bureaucracy of the organization, or organizations that feed the information to the disseminating party, may cause further vulnerabilities in of itself because of the lack of timely dissemination and distribution of information that would have otherwise, prevented such an attack from ever happening, or because the information was released too rapidly as it was not properly “sanitized” (the word “sanitizing” refers to “data sanitizing” in that critical, key information is removed for anonymity reasons, thus any individuals or organizations that could [potentially] be at risk, would not be exposed, esp. in public forums or areas of public display).

It is also possible to consider the case of potential damages and liabilities caused by any potential wrongdoings, misplaced, mismanaged or incorrect information, or information distributed in an untimely manner, raises into question by a third part or recognized member, such as another participating member of the consortium or institution, such as another government body, agency, department, or another corporation.

Despite the complexity of these liabilities, their issues and possible solutions, it may not be easily answered as to the method by which the administrative process might be handled. In addition to any potential liability or issue related to its method of dissemination or distribution of the information provided, the consortium or institution may also need to comply with either government and/or corporate compliance and/or governance requirements, particularly relevant if any such information is not sanitized or cleansed, and may contain data that would otherwise be considered harmful or extremely detrimental to the corporate entity, agency, department in question, its reputation, or even worse, its continuation and existence. Without legal and operational assurances about preventing undo harm, and at the same the preservation of the data collect, the organization would not be capable to fulfill its organizational charter since whatever, or whomever organization or organizational group in question, would have such a detrimental effect that it could reliably carry out its goal.

With the introduction of intellectual property standards (which I find continues to be an issue as to the refinement process of what definitions are what, who decides on what or who, etc.), intellectual property rights concerning the data provided by the organization may also hamper its abilities to disseminate and distribute said information. Although it is unclear as to how one might define such a conclusion; however, it may be possible to generalize that a third-party providing the electronic attack information may forego any commercial rights to it, its dissemination, and who receives it. However, the situation then becomes much like a feeding frenzy in that other interested parties might find the data or information not only useful, but valuable, thus making efforts or attempts at claiming the property as their own. This is particularly true is the entity in question foresees the ability in terms of revenue-generating capabilities, thus reinforcing the “feeding frenzy” scenario.



Conclusion

All of these circumstances may further cause delays in the abilities of the organization wishing to participate in information exchange programs through their ISAC. Further investigation of information sharing, collaboration and dissemination, and agreements in terms of the legalities of the issues outlined, may raise a flag or reason for refinement of the ISAC programs throughout the United States. In all due respect, at a federal level, the government should be driving ALL ISAC operations for ALL sectors; therefore, any aspect of who controls what and how is left up to the efforts through the governments and not through corporate interests.

Writer's Note: This subject is far from being solved or completed.

