# The Need for Information Sharing and Analysis Organizations to Combat Attacks on State and Community Public and Private Networks


## Abstract

*An ever increasing number of attacks are being reported on various city and state computer systems and networks worldwide. These attacks have resulted in the disruption of city operations or the release of personnel information. Cities and states need to protect their systems but frequently plans to do so are lacking and the ability to respond to cybersecurity events is non-existence. This is especially true for smaller communities that do not have the budget to hire full-time security personnel or contract for security services. A critical step that states and communities can take is the establishment of a state or community Information Sharing and Analysis Organization (ISAO). This paper will describe how a state or community can use the creation of an ISAO to jumpstart various aspects of its cybersecurity program, incorporating a number of established programs in a single initiative.*


## 1. Introduction

Protection of a nation's cyber infrastructures is now generally accepted to be critical to the nation's security and survival. Most nations have focused their efforts on securing the various critical infrastructures as well as government agencies and organizations. This is true in the United States where the Department of Homeland Security has spent considerable time and resources on securing the nation from a higher-level, or national level. This has left states and communities to often "fend for themselves". At the same time, for a variety of reasons, states and communities have been increasing their efforts to provide Internet access for their citizens to access various government services. This has led to the numerous attacks that communities have experienced on their computer infrastructures. Reports in the media have attested to this and local officials have recognized the growing risk to their communities. In September 2017, *Government Technology* reported that:

> *Nearly 40 percent of local government CIOs report experiencing more attacks during the last 12 months, according to a 2016 survey by the International City/County Management Association (ICMA). And the frequency is increasing too, with 26 percent of CIOs reporting an attack, incident or breach attempt occurring hourly, while another 18 percent report a cyber attempt at least daily.*
>
> *That's bad news for local governments, which have fewer resources than many larger jurisdictions to fight back. But it's especially bad for small to mid-sized cities, counties and towns, which may have only one full-time person devoted to IT — including cybersecurity — if they are lucky.* [1]

There are three important points highlighted in this statement: 1) Communities have been the target of cyber attacks; 2) The rate of attacks is increasing; and 3) Communities have limited resources to address the cybersecurity challenge.

There are various models and frameworks that have been developed to address the creation of cybersecurity programs within organizations – including communities. Similar to the point made in the quotation from *Government Technology*, small to mid-sized cities, counties, and towns who have very limited resources to devote to cybersecurity also generally don't know how to establish a viable cybersecurity program and how to utilize the models and frameworks available to them. There have been limited attempts to explain how all of these can come together to help secure a community but the recent emphasis on the value of information sharing over the last few years provides an opportunity to provide the needed impetus and roadmap for communities to establish and mature their cybersecurity programs. In particular, this paper will focus on three elements: 1) Establishment of a community Information Sharing and Analysis Organization (ISAO) and understanding the benefit of sharing across the different sectors in a community; 2) Implementation of the Community Cyber Security Maturity Model (CCSMM); and 3)

Use of the NIST Cyber Security Framework at the appropriate point in the development of the community's security program.

## 2. Information Sharing

The start of formal information sharing for cybersecurity purposes within the United States began in 1998 with the publication of the Presidential Decision Directive NSC/63 (PDD 63).[2] This directive from the White House, signed by President Clinton, was aimed at measures to better protect the critical infrastructures for the nation. One of the proposed efforts was to form Information Sharing and Analysis Centers (ISAC) for each of the critical infrastructures identified by the government. These centers were to share "important information about vulnerabilities, threats, intrusions and anomalies" within each of the sectors and to provide this information to the federal government as well. The federal government was also supposed to share information pertinent to the various critical infrastructures with each of the ISACs.

One of the initial concerns expressed by members of the various critical infrastructures, and by skeptics of the program in general, was why would organizations share information with potential competitors that might be used against them in a competitive environment? This has been overcome within the sectors as organizations have come to realize the benefit of sharing information. To illustrate the point, the financial services sector has one of the most robust and capable ISACs today. The Financial Services ISAC (FS-ISAC) has thousands of members both within the United States and abroad. If one of its members, Bank Alpha, discovers an intrusion or an attack on their systems and network, the probability that others within the banking community might also be experiencing the same attacks. Bank Beta may not have detected the attacks but if Bank Alpha shares that information with the FS-ISAC who then passes it on to all of its members, Bank Beta would be warned and would be able to determine that they too were under attack. This time it was Bank Alpha that noticed the attack first. The next time it might be Bank Beta that first notices the indications of an attack. Collectively, the banks realize that they are better off sharing information with each other.

It is important to note that in effect, the financial services community (and others) have learned that while the organization consists of a number of organizations that are in competition with each other, when it comes to cybersecurity, the banks are not competing against each other, but are competing against the cyber attackers. From the community perspective, the financial services community, working together, is competing against those that are attacking its members, and not a battle between the members themselves.

Cybersecurity information sharing took another step forward in 2015 when President Obama issued Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing. [3] This document extended the information sharing ecosystem beyond the critical infrastructures to create Information Sharing and Analysis Organizations (ISAOs) which would include any "sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities." [3] This executive order was a result of the realization that the majority of the nation did not fall into one of the critical infrastructures but would still benefit from being part of an information sharing program.

One important point in the executive order was the recognition that an ISAO could be based on a geographic region. This has led to the development of a few state ISAOs and discussions about community ISAOs. An ISAO based on a region would include members from many different sectors – both critical infrastructures as well as sectors not considered critical. The benefit of such an organization was seen in research conducted in support of efforts to define processes for community incident detection and response. Specifically, in work which led to the development of a "Honey Community." [4]

### 2.1. The Honey Community

The Honey Community was created to provide useful data on attacks that occur on a community. Instead of monitoring the networks of a real community, the researchers created a fake community and provided a website for it. The website included various sectors that are typically found in a community including such things as public utilities, local government offices, and a school district. Similar to other honey devices, it was created and then monitored for a (short) period of time. The data was then used to examine possible ways to detect an attack that was occurring on a community.

What was notable about the data gathered was discovered when looking not any one of the individual sectors but across the sectors. In the short period of time the Honey Community was available,

there were 3060 identified attacks. These occurred on one or more sectors. Of the 3060 attacks, 1430 were identified as an attack on a single sector, 151 on 2 sectors, 52 on 3 sectors, 16 on 4 sectors, and 9 on all 5 sectors. [4] This was interesting data but the researchers were surprised when they examined the data and realized that 1402 attacks would not have been identified by looking at any one of the sectors individually. These were noticed as attacks only when examined across the community. This was a significant finding because in almost all cases, individual sectors in a community (or state) confine their discussions on security events to others in the same sector or to trusted individuals known personally that may or may not be in the same sector. If the community wants to have the best chance at detecting intrusions, however, information needs to be shared across all sectors within the community.

### 2.2. The Multi-State ISAC

Some may already know about the existence of the Multi-State ISAC (MS-ISAC) and believe that it is designed to provide the information sharing needed by a community. While the MS-ISAC has a very large number of members from states and communities around the nation, they are not sufficient for all that is needed in a community. They are an important element, and communities should be members of the MS-ISAC, but there is a side of information sharing that relies on trust which is often hard to obtain in an organization such as MS-ISAC. While members trust the MS-ISAC, they may not be comfortable with other members of the organization and indeed will not know all of the members of the group. Trust can be more easily obtained through personal contact and working with individuals which a community ISAO will more easily be able to provide.

## 3. A Community Maturity Model

A problem that states and communities frequently face is not knowing where to begin in establishing their cybersecurity programs. Many community leaders are unaware of the significance and importance of such a program, but even when made aware, how to get started on one is a daunting process. One effort at making states and communities aware of the cybersecurity challenges they faced started in 2002 with the first community cybersecurity exercise. Following this first exercise, which took place in San Antonio, TX, a number of other state and community exercises were conducted. These were extremely successful in making local leadership aware of the type of issues that they faced. What they didn't do, however, and what was not realized until the communities were visited again, was the communities did not have a mechanism or plan to move the community forward. What should they do first in establishing a viable cybersecurity program? What needs to be done next? What can be postponed until the program is more mature? There were plenty of vendors willing to supply services or products but how does the community decide what is really needed at the start and what can be purchased at a later date? The monetary concerns were especially problematic as almost no community had a budget already established for implementing a cybersecurity program.

The researchers conducting the exercises took a step back at that point and developed a plan via the creation of the Community Cybersecurity Maturity Model (CCSMM). [4] This model provided three things: 1) It served as a 'yardstick' so that a state or community could measure where it was in terms of its security program; 2) It provided a roadmap for what a state or community needed to do in order to move from one level in the model to the next; and 3) It provided a common point of reference so that two communities could discuss their programs with each other and have an understanding of what each is trying to achieve.

The model addresses specific areas a community needs to improve when it comes to cyber threats. The areas of improvement are called *dimensions*. There are four dimensions identified in the CCSMM. They are **awareness, information sharing, policies** and **planning**. Each of these dimensions has five levels of maturity. The levels begin at the **Initial** level (Level 1), which is where every community begins, and builds a roadmap for communities to improve to reach a **Vanguard** level (Level 5). Level 5 is the stage where cybersecurity is a business imperative and is simply incorporated into every aspect of government, industry, and public life.

The improvements are accomplished with *implementation mechanisms*. The implementation mechanisms allow us to progress from one level to the next in each dimension. The implementation mechanisms are the activities used to:

- Increase awareness
- Establish information sharing practices
- Add cyber components to policies in a meaningful way
- Incorporate aspects of cyber security into continuity plans

The implementation mechanisms are:

- Metrics
- Processes and procedures
- Technology
- Training
- Assessments

After development of this model, the researchers proceeded to provide information on the model and how to use it to additional states and communities around the nation. It was well received and feedback from individuals indicated that it was easy to understand and follow.

The model did a lot to help provide an organized approach to cybersecurity at the state and local level. It was adopted by the National Cybersecurity Preparedness Consortium (NCPC) to organize the efforts of its members around it. The NCPC is a five university consortium dedicated to providing "research-based cybersecurity-related training, exercises, and technical assistance to local jurisdictions, counties, states, and the private sector. [5] The consortium has provided online and classroom based training to every state and territory in the U.S. and continues to develop training courses to fill in the gaps in the CCSMM where no training currently exists.

While the model has been a useful aid to states, territories, and communities it has not proven to be the catalyst that is needed to energize communities around the nation. In communities where there is a strong champion for cybersecurity who is in a position of authority, the model can serve the purpose it was designed for and the community can move forward in an organized manner to implement a viable and sustainable cybersecurity program. If there is no champion, however, cybersecurity efforts tend to languish and there will be a momentary surge in interest which then gradually gets lost in the day-to-day operational issues facing a city. Unless the city is hit with a cybersecurity event of some sort, such as ransomware or a security breach of an important system, the community is likely to continue with only minor efforts to secure their critical cyber infrastructures. What is needed is a catalyst that will inspire all communities to develop their cybersecurity programs and that provides some guidance on what needs to be accomplished. The National Institute of Standards and Technology (NIST) developed a framework with the hope that it would provide the guidance that not only federal departments and critical infrastructures could follow but that could also be utilized by industry and the nation in general. This framework is called the Cyber Security Framework (CSF)

## 4. The Cyber Security Framework

NIST published version 1.1 of what is commonly referred to as the Cyber Security Framework in April of 2018. The official title, "Framework for Improving Critical Infrastructure Cybersecurity", better describes the original focus of the document. While the original intent was to address the security of the critical infrastructures, the document is valuable for organizations in any sector. As described in the Executive Summary for the framework:

> *While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community. The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience.*
>
> *The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening cybersecurity in critical infrastructure as well as other sectors and communities.*
>
> *The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.* [6]

At the heart of the framework is a set of activities that should be considered as part of every cybersecurity program. These issues are:

1) Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2) Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
3) Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4) Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
5) Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. [6]

These five elements are referred to as Functions in the framework. They are used to organize specific cybersecurity activities at the highest level. These many different cybersecurity activities are further organized into Categories of activities with similar outcomes that fit into each Function. The Categories are further subdivided into Subcategories of "specific outcomes of technical and/or management activities." Finally the items found in the various Subcategories are provided references to the standards, guidelines, and practices that illustrate ways that the desired outcomes can be achieved. When taken in its totality, the framework provides organization to a vast amount of knowledge on cybersecurity issues.

The CSF provides a tremendous amount of useful information and for large organizations, whether in government or industry, it is a valuable tool or guide that can be used to address the key cybersecurity issues of identification, prevention, detection, response, and recovery. The key, however, is that to be able to fully utilize the CSF and to use it as guidance on what your cybersecurity program needs to include can be a daunting task often requiring individuals with a firm grasp on cybersecurity. Simply handing the CSF to an IT office in a state or community or to a small- or medium-sized business could easily lead to frustration due to the sheer volume of information contained in it. What is needed is step-by-step guidance to assist individuals in how to incorporate the information referenced and described in the CSF into their own cybersecurity program. NIST has provided additional guidance on how to implement the framework but incorporating the efforts into the other programs mentioned will better help to guide states and communities on how to ensure their programs address each activity at the appropriate point in the development of their individual programs.

## 5. The Elements of a Combined Approach

None of the programs described so far have proven to be the panacea for states and communities require to develop and sustain their cybersecurity programs. Each, for different reasons, are not individually sufficient to provide the needed guidance that will help to put a state or community on the path to develop a sustained cybersecurity program. If, however, the programs are combined in a coordinated fashion, the three requirements needed for developing a program can be realized. Specifically, what is needed (and which is provided by each) is:

1) A champion or xxxx effort that will ensure that the program does not get dropped as interest inevitably wanes. With the nature of an ISAO and with the current impetus to increase the level of information sharing, an ISAO can help ensure the program does not languish and devolve into an ineffective organization.
2) A framework that describes the areas the program needs to include and that provides guidance for where to find more detailed information about each aspect of the security program. The CSF does an excellent job in providing this information.
3) A roadmap for what needs to be done first and what can be implemented at a later time. The CCSMM was designed for this purpose and by including the other two elements into the model it can provide a step-by-step approach for a state or community to develop its sustainable cybersecurity program, keeping in mind that it is most likely the case that as the process begins, there will not be a budget to accomplish this and the steps need to begin with items that are at no or at a low cost.
4)

Currently there are a lot of discussions about the benefits of sharing cybersecurity information.

## 6. The First Step – Creating a Community ISAO

The first step will be the establishment of the Community ISAO. The Community ISAO will assist the community to stay engaged in their maturity of cybersecurity awareness, information sharing practices, cybersecurity processes and overall plans to integrate cybersecurity into their community's continuity of operations. Essentially, the Community ISAO will become the cybersecurity champion of the community.

The next step will be to define the goals and mission of the Community ISAO. Having specific goals and mission will help to drive the structure needed to accomplish the goals and provide guidance on which organizations (or members) should participate in the ISAO or where an additional ISAO will be needed. Here we will decide how far reaching the Community ISAO will extend. For example, we will need to decide the geographic scope of the organizations who can participate. Will the ISAO extend it's services to organizations within the city limits, or will counties also be included and how far out geographically will the ISAO remain effective.

Once we have established our goals and defined the potential members, we will need to implement programs and training that will encompass the varying states of cybersecurity preparedness our potential organizations may be at. This is where the CCSMM will become a key asset as it will guide the development of needed programs that will improve each organizations cybersecurity posture in awareness, information sharing, processes and planning. Essentially, the CCSMM will be the mechanism the ISAO will use to develop programs that will assess what level of capability an organization is at and will provide the roadmap needed to improve the organization's overall cybersecurity. Enhancing each organization's cybersecurity posture will improve the overall community cybersecurity preparedness.

An ISAO will help by keeping people talking about cybersecurity

Discuss public private partnership

## 7. Integrating the CCSMM

Using the CCSMM to assess a member organization's overall cybersecurity maturity will classify each organization to be at a level 1 thru 5 as previously mentioned. Once an organization's level is determined, the Community ISAO can develop a plan for the organization. If for example an organization is assessed as a level 1, cybersecurity awareness training, information sharing practices, the appropriate level of NIST practices can be shared which will include continuity of operations plans.

## 8. Incorporating the NIST CSF

NIST CSF must be implemented based on an organization's capabilities. By using the CCSMM to determine the level of the organization, the appropriate NIST guidelines can be recommended.

## 7. Summary

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance

## 10. References


[1] Tod Newcombe, "Small Towns Confront Big Cyber-Risks", *Government Technology* (online), http://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html, October/November 2017.

[2] Bill Clinton, "Critical Infrastructure Protection", Presidential Decision Directive /NSC 63, May 22, 1998.

[3] Barack Obama, "Promoting Private Sector Cybersecurity Information Sharing", Executive Order 13691, February 20, 2015.

[4] K. Harrison, J. Rutherford, G. White, "The Honey Community: Use of Combined Organizational Data for Community Protection", HICSS-48, Kauai, HI, January 7, 2015

[5] G. White, "A Grassroots Cyber Security Program to Protect the Nation", HICSS-45, Maui, HI, January 4-7, 2012.

[6] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.0,416 2018.pdf