ISAO 200-1

Foundational Services and Capabilities

Draft Document—Request for Comment

ISAO SO—2017 v0.1

ISAO Standards Organization

October 30, 2017

Acknowledgments

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from the private, professional, and government communities in an ongoing effort to produce a unified voluntary set of guidelines for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization

Gregory B. White PhD
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Larry Sjelin
ISAO SO Chief of Staff
Center for Infrastructure Assurance and Security, UTSA

Working Group 2—ISAO Capabilities

Nick Sturgeon
Security Operations Center Director, Pondurance, LLC
Vice President Cyber Leadership Alliance

Jill Fraser
Chief Information Security Officer
Jefferson County, CO Information Technology Services

The ISAO SO leadership and authors of this document also would like to acknowledge those individuals who contributed significantly to the development of this publication, including the following:

Elyse Goldenberg, LMI; Terry Leach, Agrepedia; Alelie Llapitan, President and Co-Founder, Solutionize; Chris Needs, NC4; and David Sula, Co-Chair of Working Group 7.

Special thanks from the authors go to the ISAO SO advisors and staff who provided amazing support and guidance in the development of this document: Josef Klein, James Navarro, and Allen Shreffler.

Table of Contents

Revision Updates

Item	Version	Description	Date
1	0.1	Initial draft publication	

1 Executive Summary

Building a new Information Sharing and Analysis Organization (ISAO) can be very challenging. There are multiple complexities to overcome before the ISAO can become operational. Many of these issues were addressed in ISAO 100-2, "Guidelines for Establishing an Information Sharing and Analysis Organization," which was published October 14, 2016. ISAO 100-2 introduced an initial set of guidelines for establishing an ISAO, with the purpose of providing guidance to those looking to establish an ISAO or to those newly formed ISAOs. The 100-2 document introduced a list of services and capabilities that ISAOs perform. Those services and capabilities were categorized into "Foundational," "Advanced," and "Unique." The Capabilities and Services Working Group (WG2) felt that it would be beneficial to expand on those services and capabilities outlined in Appendix A of ISAO 100-2. As a result, WG2 will develop a series of three documents covering the foundational, advanced, and unique services and capabilities. The outcome of these documents is to assist the ISAOs so they can provide immediate value to their membership.

2 Introduction

Appendix A of the ISAO100-2 publication introduced a list of services and capabilities that ISAOs offer and perform. Those services and capabilities were categorized into Foundational, Advanced, and Unique. The purpose of this document is to assist ISAOs by providing a comprehensive review of the foundational services and capabilities of an ISAO: collection and dissemination, facilitate member sharing, analyze information, and surveying members. This in turn will give ISAOs a deeper understanding of how they can operationalize the technical, analytical, and personnel that are built around those capabilities and services. The structure of this document is framed to begin with the easier, and then implemented to the more challenging capabilities and services. This will facilitate a natural progression for those ISAOs that are further along in their evolution to navigate to the area within the document that is appropriate for their current situation. Additionally, collection and dissemination have been split as separate services and capabilities, and thus each will have its own chapter. After evaluating the processes and technologies for collection and dissemination, WG2 felt that each was distinct enough to be independent services and capabilities. Future documents will focus on the Advanced and Unique capabilities and services identified in ISAO 100-2.

3 Member Surveys

3.1 Introduction

Surveying members is a key way of obtaining an understanding of the member's needs and evaluating how you are meeting those needs. A survey is defined as "the selection of a relatively large sample of people from a predetermined population (the "population of interest"; this is the wider group of people in whom the researcher is interested in a particular study), followed by the collection of a relatively small amount of data from those individuals (Kelley, Clark, Brown, & Sitzia, 2003)." Surveys are conducted as a part of descriptive research. They enable organizations to get feedback about specific products or programs, as well as more general input into an organization's mission or objectives. Surveys can be used in determining how the other four foundational capabilities and services are designed and implemented. There are several ways to survey members. Organizations are free to choose what is most appropriate for them, or to develop their own method of surveying members. When choosing to conduct a survey, it is can be easy to design a survey that will provide poor-quality results. There are several steps involved in designing a survey that will produces high-quality results.

First, know what you are trying to accomplish with the survey. There should be a clear vision to what the purpose of the survey. This is done by clearly defining what information or knowledge you are trying to gain from your members? The questions should be specifically designed to pull that information from the respondents.

Second, identify who the target audience will be. You will not get useful input if you ask physical security specialists questions on advanced cyber-security issues. Likewise, polling executives only will likely end up with different results than polling the membership at large. Knowing who the right community is, for the specific topics you want input on, will yield the most useful and valuable results.

Third, when developing the survey, you should have a good understanding of the overarching questions you are trying to answer. The specific survey questions will need to be designed to ensure that you are collecting the right data. The way the questions are worded, ordered, structured, and sequenced can have a major impact on how they are answered.

Finally, it is important to understand the best method of reaching the target audience. There are a few different types of surveying methods, including phone conversations, online surveys, and face to face. You want to use the method that will get you the best results based on the preference of the ISAO membership base. Additional details about the different survey methods will be discussed in a later section.

3.1.1 Qualitative, Quantitative, and Mix Methods

There are three different types or approaches when it comes to research that can be applied to surveys: qualitative, quantitative, and mix methods. Qualitative research is used to explore the meaning of individuals or groups and is done usually done by gathering non-numerical data

(Creswell, 2009). Quantitative research can be used to gather opinions and trends in thoughts and take a deeper look into a problem. Quantitative research is "a means for testing objective theories by examining the relationship among variables" (Creswell, 2009). This is done by gathering numerical data, it is easier to analyze, and it is descriptive. Quantitative research uses more structured collection methods than qualitative and is used to turn the gathered data into usable statistics. The mix method approach combines both quantitative and qualitative in the same study/survey (Creswell, 2009). There are three types of mix methods: sequential mixed methods, concurrent mix methods, and transformative mix methods. The end goal and the means by which the data will be collected will determine the best method to use (see Table 1).

Table 1. Quantitative, Mixed, and Qualitative Methods (Creswell, 2009)

Quantitative method	Mixed method	Qualitative method
Predetermined	Both predetermined and emerging methods	Emerging methods
Instrument-based questions	Both open- and closed-ended questions	Open-ended questions
Performance data, attitude data, observational data, and census data	Multiple forms of data drawing on all possibilities	Interview data, observation data, document data, and audio-visual data
Statistical analysis	Statistical and text analysis	Text and image analysis
Statistical interpretation	Across database interpretation	Themes, patterns interpretation

3.1.2 Advantages

There are several advantages for why an ISAO would conduct a survey of its membership:

1. It can be developed in a short amount of time.
2. It produces data based on real-world observations (Kelley et al.).
3. It can produce data that reflect the larger population (Kelley et al.).
4. It can produce large amounts of data in a shorter time span (Kelley et al.).
5. It provides a mechanism for the membership to gain buy-in to the ISAO.
6. It provides a mechanism for the membership to provide meaningful input.

3.1.3 Disadvantages

There are several disadvantages of conducting a survey:

1. It can be time-consuming.
2. Response rates can affect the significance of the data.
3. The significance of the data can be negatively affected if the questions are too focused on the range of coverage (Kelley et al.).
4. The data may lack detail or depth on the topic being investigated (Kelley, Clark, Brown, & Sitzia, 2003).
5. Survey participation is a challenge.

3.2 Survey Methods

ISAOs can design several types of survey methods to post to their membership. The following section discusses several of those methods. During the process of selecting a specific method, there are other factors to take into account. As mentioned above, several elements in the survey design will have a direct effect on the survey's outcome. When designing a survey, there are three principles to follow: Principle of Wording, Principle of Measurement, and General Appearance (Sekaran & Bougie, 2009). One important advantage of implementing these principles is that bias is minimized. Once the method and design of the survey are complete and the development of the specific questions has started, there are 11 elements to take into account (Sekaran & Bougie, 2009):

- Language and wording of the question
- Open-ended questions vs. closed-ended questions
- Positively and negatively worded questions
- Double-barreled questions
- Ambiguous questions
- Recall-dependent questions
- Leading questions
- Loaded questions
- Social desirability
- Length of the questions
- Sequencing of the questions.

Note: In addition to the advantages and disadvantages listed above, each survey method may have its own unique or additional advantages or disadvantages.

3.2.1 Postal Questionnaires

In general, the questionnaire method is best used when there is a specific question to be answered and when there is a known measure of the variables of interest (Sekaran & Bougie, 2009). There are a couple of different means to deliver questionnaires, mail or web based. A disadvantage of this method is the low response rates, which in turn requires a larger sample size. An advantage of postal questionnaires is that they are usually more cost-effective and less time-consuming (for both the researcher and the respondent), anonymity is high, and it's a very efficient means to collect data. With this method, a 30 percent response rate is considered a satisfactory rate (Sekaran & Bougie, 2009), and the design of the questionnaire is extremely important.

3.2.2 Web Based/Electronic

The most obvious way to survey members is to create an actual survey using a survey website. Under this method, an organization identifies a specific set of questions it wants its members or partners to answer, and it places those questions into an online survey functionality. The advantage of this method is that the organization can send the survey to specific people

electronically or to a large group of people, the surveys are very inexpensive and easy to administer, there is fast delivery, and all the responses are captured in one place for review and analysis (Sekaran & Bougie, 2009). One of the biggest advantages to web-based surveys is there often is the ability for members to participate in online survey without attribution, so they may be more likely to be willing to provide honest input. Disadvantages include requiring Internet connectivity, respondents must be willing to take the survey, and requiring a large sample population (Sekaran & Bougie, 2009). Examples of web-based survey tools include Survey Monkey, SurveyGizmo, Google Forms, Typeform, SurveyLegend, and Polldaddy (*note*: these are not recommendations of these products).

3.2.3 Telephone Interviews

Another way to survey members is through individual one-on-one phone calls. This is the most time-consuming method but also has the potential to provide the most useful feedback. It is important to ask all members the same questions during the survey, but one-on-one conversations can enable an organization to engage in specific topics in more detail. This detailed information can provide additional useful context and ideas and can lead to a clearer understanding of a member's needs. The individual contact is also an excellent way to build relationships with members. Telephone interviews can be conducted through computer-assisted telephone interviews (CATI), which are easy to use and manage (Sekaran & Bougie, 2009). Another advantage of using CATI is that the interviews gather more accurate data and provide faster analysis. Some disadvantages are that non-verbal cues cannot be read and that the interviews have to be kept short (Sekaran & Bougie, 2009).

3.2.4 Online Webinar

A third method of surveying members is through a common webinar or group call. Under this method, members are invited to attend a single call or webinar with other members to respond to your survey questions. This has the advantage of saving time, there are no individual phone calls, but it can be less effective in gaining feedback as members might be reluctant to speak honestly with others on the call. Similarly, one company or person who provides constant feedback on the call might dominate the discussion and skew the input. However, having multiple members discuss the survey on a common call can also lead to an effective "brain storming" session where individual ideas are explored in more detail among the group.

3.2.5 Face-to-Face Interviews

This survey method involves the ISAO conducting face-to-face interviews. These interviews can be either structured or unstructured. For unstructured interviews, there is no planned sequence of questions. Structured interviews are when there is a known set of what data and information is needed and there is a predetermined set of questions (Sekaran & Bougie, 2009). Face-to-face interviews could involve the ISAO conducting the interview at the ISAO's office, its member's office, or other locations. An advantage of this method is that the response rate is higher than other methods—due to the fact that the ISAO can sell the survey to the individual members (Kelley, Clark, Brown, & Sitzia, 2003). Before deciding to conduct a face-to-face interview,

consider the advantages and disadvantages. The biggest advantage to face-to-face interviews is that the interviewer is able to pick up on nonverbal cues and body language. These cues could show whether or not the respondent understands the questions. Face-to-face interviews also allow the respondents to clarify any of the survey questions they do not understand (Sekaran & Bougie, 2009). There are a few disadvantages to face-to-face interviews: they are time-consuming, there are geographic limitations, interviewer bias can affect how the response is interpreted, and there's the cost for interviewer training (Sekaran & Bougie, 2009).

(See Appendix A for examples.)

3.3 Chapter Summary

Surveys can be a powerful tool that will allow an ISAO to collect a large amount of data in a short amount of time. This information can be used to understand how their products and services are being received by their membership, can be used to determine future direction of the ISAO and give the membership an opportunity to be engaged with the ISAO. Each survey method has its own advantages and disadvantages. When selecting which survey method to be utilized it is important for the ISAO to take into account the challenges, limitations, expected outcomes and benefits of conducting a survey. As noted, the above represents some ideas and methods and ISAO can use to survey their members. Organizations are encouraged to adopt whatever methods work for them. As with most initiatives, there will be some trial and error involved as organizations learn how best to engage with their members.

4 Collection

4.1 Description

The goal of this chapter is to assist ISAOs in understanding the operational, technical, analytical, and personnel capabilities for the collection of cybersecurity threat information (CTI). As defined by National Institute of Standards and Technology (NIST) SP 800-150, "Guide to Cyber Threat Information Sharing," CTI includes "indicators of compromise, tactics, techniques, and procedures used by threat actors," as well as any information that an organization can use to "identify, assess, monitor and respond to cyber threats (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016)." These data can come from a variety of sources: sensors, by scrapping open-source reporting, from sites such as cybersecurity vendors, media articles, cybersecurity blogs, white papers, other ISAO or ISACs, government sources, reports, and directly from the ISAO's members. Collection of CTI is one of the most important services and capabilities that an ISAO performs. According to NIST, organizations "should identify tools, sensors, and repositories that collect, produce, or store cyber threat information (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016).

4.2 Advantages

- There are a large number of closed and open sources to pull from.
- Collection from outside sources can enrich existing internal information to make it more actionable to the ISAO (Johnson, Badger, Waltermire, Snyder, & Skorupka, 2016).
- By providing a centralized resource for its membership, the ISAO can reduce costs.
- Collecting information from multiple sources, this service and capability can provide the ISAO with a better understanding of the threat landscape.

4.3 Challenges

- There is a large number of products to choose from.
- Vetting and trust of open-source feeds is an issue.
- There is an extremely large volume of data to sort through.
- There is a high rate of false positives.
- Depending on the level of data desired, the format, and the frequency of dissemination, the process may require talent, time, process, and technology.
- Finding a format that is easy for members to use and determining what is relevant or desired by membership can also take time and understanding of the constituents.
- The technology, services, and methods can be expensive.

4.4 Sources and Methods

The number of different sources and methods for collecting data can be overwhelming for new ISAOs. The best approach is to start small and only choose a few sources and methods first. Only after getting those set up and verifying that the information is providing the desired value,

should you consider adding additional sources or methods. This section will cover ways to vet sources and list how to collect information.

4.4.1 Sources

Data sources or feeds can come from either internal or external sources. First, identify what information is important. From there, identify which systems or sources contain that information:

- Emails
- Router, firewall, Wi-Fi, remote services (such as remote login or remote command execution), and Dynamic Host Configuration Protocol server logs
- Diagnostic and monitoring tools
- OS and application settings and system logs
- Anti-virus and web browsers
- Security incident and event management systems
- Help-desk ticketing systems and incident management systems
- Forensics tools
- Threat intelligence feeds.

4.4.2 Formats

There are several types of "standardized" formats for sharing indicators of compromise. Appendix C references a list of formats. An ISAO may choose to ingest all, some, or none of these formats, depending on what works best for its membership. As a note, the US-DHS Automated Indicator Sharing Program uses the STIX\TAXII format.

4.4.3 How to Collect

There are several methods for collecting data. Depending on the maturity level of the ISAO, some of these methods will be more advanced. The purpose for listing the methods here is for general awareness, although understanding these methods early in the planning stages may help with the strategic development of the ISAO. These methods include the following:

- Internal sources
- Emails
- Scripts
- Human to human
- Web spiders (United States Patent No. US 2002/0038430 A1, 2002)
- Multimedia capture and indexing (United States Patent No. US 2002/0038430 A1, 2002)
- OCR scanning (United States Patent No. US 2002/0038430 A1, 2002)
- Tools
- Automated technologies
    - STIX\TAXII
    - HITRUST cyber threat exchange

- Other resources.

4.4.4 Vetting and Validation of Sources

It is very important that members of the ISAO can trust the information, alerts, and notifications they receive. This requires that the methods, means, and sources be vetted by the ISAO. There could be considerable doubt placed on the information shared by the ISAO if the sources are questionable. ISAOs should evaluate and vet their sources of information, including their partner organizations. This section discusses ways to vet data sources and help ensure high integrity and fidelity of the information collected.

When it comes to vetting a data from a new open source, there are several considerations: First, who is contributing to that source? Second, which systems are contributing information? Third, what is the process to contribute to that source? Finally, what is the context of the data?

1. One of the first ways to vet an open-sourced data feed is to ask other ISACs and ISAOs.
2. Connect to the data feed and conduct an audit of the feed. Check for false positives and false negatives.
3. Develop a process and standard procedure for sanitizing the information collected.
4. Conduct random audits and set periodic reviews of the data feed.
5. Develop a reputation or confidence score for the data feeds.
6. Develop a process for members to rate and comment on data feeds. These reviews can be used to determine the reputation and confidence scores.
7. When considering collecting information from another organization, it may be prudent to establish a data-sharing agreement, memorandum of understanding, or non-disclosure agreement.

4.5 Post-Collection Steps

Some organizations have proven guidance for the process of collecting data. One such organization is NIST. This guidance can be found in NIST Special Publication 800-150, which provides steps on how to consume and use indicators of compromise from external feeds. These steps are validation, decryption, decompression, content extraction, prioritization, and categorization. ITIL has a similar process for incident management that can be used post-collection: identification, logging or registration, prioritization, initial diagnosis, escalation, investigation and diagnosis, resolution and recover, and closure. These processes provide a workflow for how the ISAO can handle data in collection and in analysis and dissemination.

4.6 Collection Tools and Resources

ISAOs have a considerable amount of tools and resources available to them. Some of these tools are completely free to use, some require only a one-time payment, while others require a subscription (monthly or yearly). A list of tools and resources can be found in Appendix C; it is not an all-inclusive list and is not an official endorsement of the products. The list is to illustrate some of the tools and resources that are available for ISAOs to explore.

4.7 Chapter Summary

The process of collection, as mentioned previously, is one of the most important and fundamental services an ISAO offers to its membership. As a core competency, this service should be planned out and implemented carefully. When starting out, it is important to choose one or two methods, tools, and sources to get a baseline prior to adding on more. Starting out with too many methods, tools, and sources can complicate the process and in turn reduce the level of service that the ISAO can provide to its membership. It is important to start small, concentrating on collecting information from a few known and trusted sources.

5 Analyze Information

5.1 Introduction

The second fundamental service and capability of an ISAO is "analyze information." Even at the most basic level, there are different ways to analyze cyber threat information. This process can come in the form of having a system, tool, or human conduct an analysis on data sets. This chapter of this document will not delve very deep in to this foundational service and capability. For additional information, please refer to the ISAO 700-1 "Introduction to Analysis" document. The purpose of the document is to introduce information analysis to ISAOs and provide members with a foundation for organizations attempting to understand information analysis as it pertains to ISAOs. The document will establish a conceptual framework for the analytical process including establishing requirements, collecting relevant data, processing and exploiting the data, analyzing results, and generating products to support internal and external sharing of the findings.

It is important to mention in this document a couple of important aspects about information analysis. First, this process can be time-consuming and can require a special skill set to be accomplished correctly. Second, through the analysis process, the ISAO should produce actionable information for members in the form of lessons learned, threat warnings, and trends analysis. An example of the analysis process providing actionable information can come in the form of the ISAO identifying a pattern of reconnaissance attempts of multiple member networks and as a result issuing a notice to all members, warning of a possible targeted campaign, and providing guidance on how to identify the threat. The greatest value an ISAO can provide to its membership can be in its analytical processes.

5.2 Advantages

Participation in an ISAO analysis organization allows members to pool both their data and their resources, increasing the amount of information available for the analysts to review, and it enables them to obtain a broader view of the threat environment. Generally, with more data feeds coming from the ISAO members, it can be easier to develop trends and correlations. Additionally, supplying relevant analysis makes information and situational awareness more efficient. The information gleaned from an affective analysis can add an extreme amount of value that the ISAO provides to its members.

5.3 Challenges

Members can face numerous difficulties when it comes to participation in an organizational analysis effort. From a manpower perspective, training or hiring competent analysts can be expensive, and increases in requirements and amounts of data will only increase the personnel requirements. Individually, members may be unwilling or unable to provide some data sets to the organization due to concerns about compromising proprietary data or potentially revealing information that could be detrimental to the member organization.

5.4 Chapter Summary

This particular foundational service and capability is very important. Effective analysis can provide the ISAO membership with timely and actionable intelligence. However, poor analytical skill and processes can be a major risk to the ISAO. For more details and a deeper look into the analysis process, please refer to ISAO 700-1, “Introduction to Analysis.”

6 Dissemination of Information

6.1 Introduction

Dissemination is defined as "the act of spreading something, especially information, widely" (Oxford Dictionaries). Sharing information is done to create value among ISAO members. It enables organizations to receive current news and communications that may have an impact on their business.

There are several ways to disseminate information and several types of information that could be distributed. To ensure information is both timely and relevant, members should work with their ISAO to establish mechanisms for information sharing and identify the type and frequency of information to be shared. The possible reasons for sharing information include eliciting immediate action, promoting behavior change, requesting support, and educating on a specific topic or situation. The follow sections provide additional details about the different information-sharing considerations.

6.2 Advantages

There are a few advantages of properly disseminating information:

- Alerts and advisories provide members with time-sensitive awareness of recent and active incidents, threats, and reported vulnerabilities.
- An improved understanding of the threat environment can help an organization with prioritizing its cyber-security resources.
- Specific topics can be shared that facilitate partnership building, increase knowledge of community members through training communication, or create an avenue for members to request assistance from others within their ISAO community.

6.3 Challenges

There are several challenges to overcome when disseminating information:

- Members may not see the value of time-sensitive products.
- Creating actionable products may require an operational background, which can be hard to attract, retain, or fund.
- An unfiltered flow of content could lead to information fatigue and overwhelm members, thereby reducing readership and value.
- Depending on the level of data desired, the format, and the frequency of dissemination, the process may require talent, time, process, and technology.
- Security and control must be maintained as the information is redistributed.

- The cost, level of effort, and resource needs for creation, management, and sustainment may be high, particularly to meet urgent deadlines.

6.4 Implementation Guidelines

6.4.1 Dissemination Methods

There are several types of information-sharing methods that ISAOs can use to distribute information to their membership without much technical setup:

- Telephone
- Email (broadcast or ListServ)
- Computer scripts
- In-person
- Website.

Each method has its own specific advantages and disadvantages. ISAOs are not limited to only implementing one type of method. Having redundant methods is suggested, especially for the purpose of continuity of operations.

6.4.2 Dissemination Content

There are several types of content an ISAO could distribute to its membership. Good and meaningful distributed content provides the greatest value to the ISAO membership. The following are various types of content:

- Alerts and advisories
- Regular publications
- Regular reports
- Training opportunities
- Requests for help or information
- Education, training, and awareness to ISAO members
    - Webcasts
    - Onsite/in-person
    - Online resources.

As with the different methods for dissemination, each format has its advantages and disadvantages. However, no matter which format is chosen, a couple of things to keep in mind are the spamming affect and alert fatigue. The rate at which information is disseminated to the members should be based on the impact, urgency, and importance of the information. A potential strategy to consider is a push-pull method—an example of this is an item that requires an immediate response or action to be taken, pushing the information out via an email or alert notification. For the informational-only items, post those things to a shared drive, website, or common area, where the members can pull that information down at their convenience.

6.4.3 Dissemination Format

Providing information in an easily digestible format can support the ISAO membership obtaining the most value from the information. The following are considerations regarding format:

- A brief overview of the information
- Identifying urgency and criticality
- Recommending response actions and best practices.

6.4.4 Additional Dissemination Considerations

There are a number of additional considerations an ISAO should review:

- Encryption
- Storage and retention periods
- Frequency
- Traffic Light Protocol (TLP) for handling and redissemination.

6.5 Chapter Summary

There are a few important aspects to take into consideration when building up this capability and service. First, similar to collection and analysis, there are a large number of tools and means to disseminate information. It is necessary to start out with a few simple means to disseminate information to the ISAO membership. Second, ensure that the information is being sent out in a timely manner. Third, not only does the information need to be timely, it also needs to be actionable. Fourth, it is important that the format of the information be in a consistent format, written professionally, and the material geared to the proper audience. Last, it is important to consider the sensitivity of the information, how it is to be handled, and how long the receiving party should retain it.

7 Facilitating Member Sharing

As defined in publication 100-2 (Appendix A), facilitating member sharing is the process of enabling members to share information, with or without attribution, with each other and with the ISAO. In short, the most important outcome of an ISAO in this service and capability is to facilitate and maintain trust among its membership. If the members of the ISAO community are familiar with each other, then creating trust is easier. This chapter discusses the foundational principles for an ISAO to facilitate sharing among its members.

7.1 Advantages

As stated in the introduction to this chapter, an ISAO facilitating member sharing has many advantages. The ISAO becomes the trusted and neutral medium for its members to share cyber-threat information and other potential sensitive data.

7.2 Challenges

As with the other foundational services and capabilities, there will be challenges that ISAOs face in operationalizing this service and capability. The first challenge is in creating a trusted environment. This is very challenging for an emerging ISAO, the primary reason being that members within the community may be unfamiliar with each other. A second challenge is in creating a secure environment (if desired). The process and technology required for creating a secured environment is expensive. For an ISAO just starting out, finances will probably be limited. The third challenge, if required, is creating an anonymous environment, and this challenge also is expensive. The fourth challenge will come about if one of the members violates the trust. Creating trust among the membership can take a considerable amount of time to build, but it can be destroyed in an instant. Finally, getting members to share and simply participate is also a challenge. There are many reasons why a member would not to share or participate: It can come down to the processes to share are too cumbersome, the membership does not see the value in sharing, or there's simply a lack of caring.

7.3 Methods for Implementing Facilitating Member Sharing

There are several basic methods that an ISAO can use to facilitate information sharing among its members. Many technologies that support this foundational service or capability are not cost-prohibitive. Using cloud or other online services at the beginning will not only help in cost savings, but will allow for a quicker ramp-up time for the ISAO to start delivering these services and capabilities.

- Creating email list serves is a quick and easy approach for an emerging ISAO to implement this service and capability.
- Creating or using a standard sharing protocol like TLP is an easy way to get members to agree to sharing.

- Requiring a document such as an NDA can also be very simple and can help engender trust.
- Requiring a memorandum of understanding (MOU) between the ISAO and members can be helpful. A MOU is a document that outlines the intent of action. It is not necessarily a legally binding document, but it can be helpful in defining expectations.
- Communicating the value of how sharing enhances situational awareness across the constituency can inform risk-based decision making.
- Developing multiple channels to communicate with the membership can be useful. Examples include creating weekly or monthly newsletters and holding monthly or quarterly briefings. These briefings can rotate from one member's office to the next.

7.4 Chapter Summary

The ability for ISAOs to support, encourage, and facilitate their members to interact with one another is a key indicator in how successful the ISAO is. Once all of the technologies are in place and running as designed, the success of the program will be determined by how engaged the ISAO membership is. The ISAO's leadership and staff (if available) need to be constantly communicating with its members. This interaction will help keep the membership involved. This will also go to build and maintain trust between the ISAO and its members as well as among the members.

Appendix A. Survey Example

Survey Example 1
The information from this survey will be used to improve future events.

1) **Overall, how satisfied are you with the ISAO**:

□ Excellent □ Very Good □ Good □ Fair □ Poor

2) **How useful did you find the information from the ISAO**:

Home:	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor
Work:	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor

3) **Rate the overall service of the ISAO:**

□ 1 □ 2 □ 3 □ 4 □ 5

4) **How actionable is the information from the ISAO:**

□ Extremely Good □ Very □ Good □ Poor □ Extremely Poor

5) **Is the information disseminated in a timely:**

□ Yes □ No

6) **Are you representing a Business or Individual**

a. If business, what industry: □ Finance □ Education □ IT □ Manufacturing
□ Government □ Health □ Other: _____

b. Size of company □ Small (50 or less) □Medium (51 to 249) □ Large (250+)

7) **Which method do you prefer to receive information?**

□ Twitter □ Friend □ Website: _____
□ Facebook □ LinkedIn □ Other: _____

How would you rate the different methods?

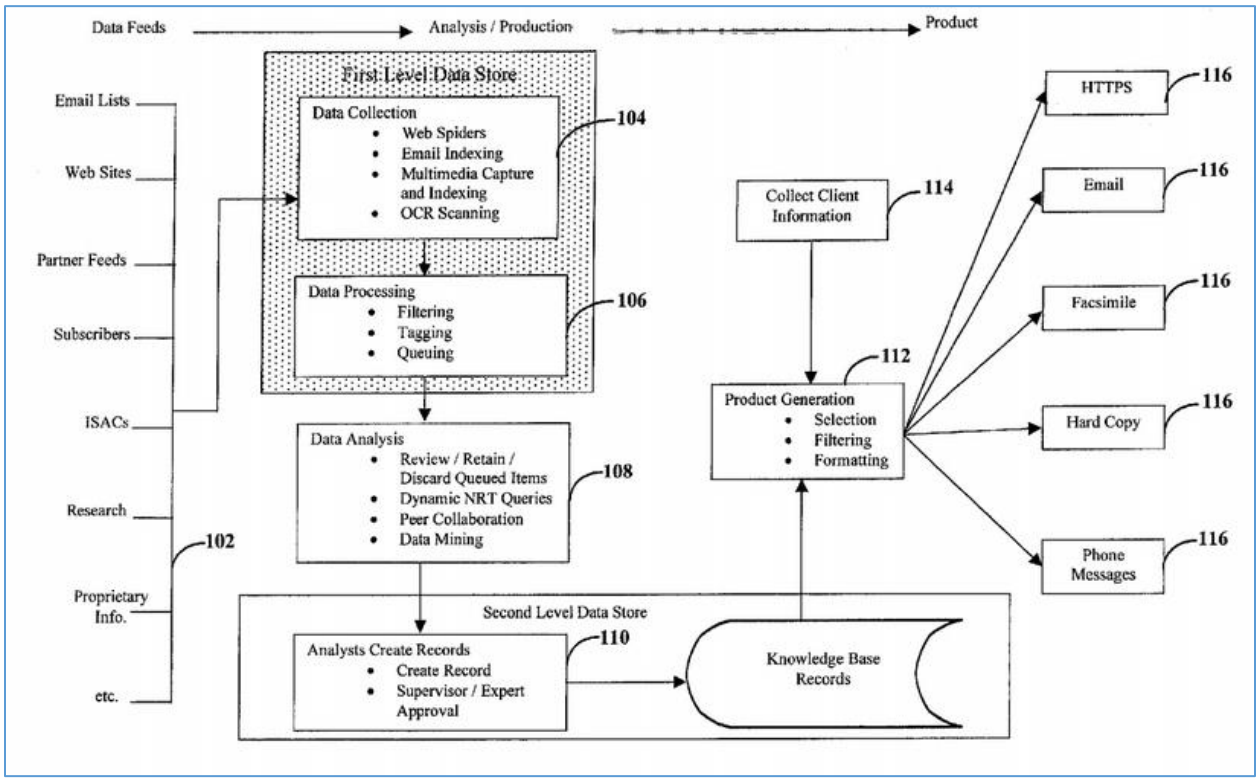
Twitter	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor
Email	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor
Automated	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor
Web Alerts	□ Excellent	□ Very Good	□ Good	□ Fair	□ Poor

Interested in signing up for Cybersecurity News & Alerts?
Leave your contact information below.
Name:_____
Email:_____

Comments or Suggestions?
_____
_____
_____

Appendix B. System and Method for Collection and Analysis

Figure B-1. System and Method for Collection and Analysis



(United States Patent No. US 2002/0038430 A1, 2002)

Appendix C. Standardized Formats

Table C-1. List of Standardized Formats

Format	Description
CAPEC	The objective of the Common Attack Pattern Enumeration and Classification (CAPEC™) effort is to provide a publicly available catalog of common attack patterns classified in an intuitive manner, along with a comprehensive schema for describing related attacks and sharing information about them (https://capec.mitre.org/about/index.html).
CybOX	Cyber Observable eXpression (CybOX™) is a standardized language for encoding and communicating high-fidelity information about cyber observables (http://cyboxproject.github.io/about/).
IODEF (RFC5070)	The Incident Object Description Exchange Format (IODEF) defines a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams about computer security incidents (http://cyboxproject.github.io/about/).
IDMEF (RFC4765)	*Experimental*. The purpose of the Intrusion Detection Message Exchange Format (IDMEF) is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them (https://tools.ietf.org/html/rfc4765).
MAEC	Malware Attribute Enumeration and Characterization (MAEC™) (pronounced “mike”) is a community-developed structured language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns (http://maecproject.github.io/about-maec/).
STIX	Structured Threat Information Expression (STIX™) is a structured language for describing cyber-threat information so it can be shared, stored, and analyzed in a consistent manner (http://stixproject.github.io/about/).
TAXII	Trusted Automated eXchange of Indicator Information (TAXII™) is a free and open transport mechanism that standardizes the automated exchange of cyber-threat information (http://taxiiproject.github.io/about/).
VERIS	The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges in the security industry—a lack of quality information (http://veriscommunity.net/index.html).

Appendix D. Tools and Resources

Table D-1. List of Tools and Resources

Name	Type	Link
Ransomware Tracker	Resource—feed	http://ransomwaretracker.abuse.ch/blocklist/
Github	Resource—feeds and tools	https://github.com
Cymon	Resource—feed	https://cymon.io/
SANS ICS Suspicious Domains	Resource—feed	https://isc.sans.edu/suspicious_domains.html
Spamhaus	Resource—feed	https://www.spamhaus.org/
PasteBin	Resource—feed	https://pastebin.com/
Threatglass	Resource—feed	http://www.threatglass.com/
VirusShare	Resource—feed	https://virusshare.com/
AlienVault	Resource—feed	https://www.alienvault.com/
ActorTrackr	Tool	http://actortrackr.com/
AIEngine	Tool	https://bitbucket.org/camp0/aiengine
Automater	Tool	http://www.tekdefense.com/
CrowdFMS	Tool	https://www.crowdstrike.com/